Access Point Controller

Compex APc User Manual

Version 1.05

Copyright

This document contains information, which is protected by copyright. Reproduction, adaptation, or translation without prior permission is prohibited, except as allowed under the copyright laws.

© Copyright 2015 Compex Systems Pte Ltd.

All Rights Reserved.

Feedback

Please direct any comments or suggestions about this document to: feedback@compex.com.sg

Trademark Information

Compex® is a registered trademark of Compex Systems Pte Ltd. Microsoft Windows and the Windows logo are the trademarks of Microsoft Corp. All other brand and product names are trademarks or registered trademarks of their respective owners.

Disclaimer

Compex provides this manual without warranty of any kind, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Compex may make improvements and/or changes to the product and/or specifications of the product described in this manual, without prior notice. Compex will not be liable for any technical inaccuracies or typographical errors found in this guide. Changes are periodically made to the information contained herein and will be incorporated into later versions of the manual. The information contained is subject to change without prior notice.

Publication date and software version

Published 25 February 2015. Software version 1.05. Manual version 1.05.3.

Table of Contents

Copyright....2

ChangeLog....6

Section 1: Overview of the AP Controller....10

1.1 Features....10
1.1.1 Discovery....10
1.1.2 Management (Monitoring)....10
1.1.3 Management (Changing the Settings of Devices)....10
1.1.4 Users....11
1.1.5 Firmware Upgrade....11
1.1.6 Nagios based monitoring....11
1.2 Hardware and Software Components....11
1.3 Licensing....12
1.4 Layout of this Manual....12

Section 2: Getting Started with the APc....13

2.1 Download the .iso File....13
2.2 Installing the .iso File to a PC – Initial Step....13
2.2.1 Using a DVD Optical Drive to Install on a PC....13
2.2.2 Using a USB Flash Drive to Install on a PC....13
2.3 Installing the .iso File on a Virtual Machine – Initial Step....15
2.3.1 Create the VM....15
2.3.2 Settings for the VM....15
2.3.3 Note for VMware....15
2.4 Installing the .iso File – Subsequent Steps....15
2.5 Perform Initialization by Running Three Scripts....22
2.5.1 Run the Script for 'apc'....22
2.5.2 Run the Script for 'mysql'....23
2.5.3 Run the Script for 'ftp'....25
2.6 Logging in to the APc....26

Section 3: Creating an APc Network on the [Create Network] Page....28

Section 4: APc Network Settings in the [Network] Page....30

Section 5: Adding APs and using the [Discovery] Page....31

5.1 Configuring the APs....31
5.1.1 Troubleshooting Steps if the L2TP Tunnel is Not Working
....33

5.2 Adding APs....34
5.3 Using the [Discovery] Page to add APs....34
5.3.1 AP SNMPv3 Settings....35
5.3.2 Scan IP Range....35
5.3.3 Note on the Scanning Time....36
5.3.4 The Devices Table....36
5.3.5 The Mode / Status icon....37

Section 6: The [Management] Page....38

6.1 The Export / Import / Create AP Tabs....39
6.1.1 The Export AP(s) Tab....39
6.1.2 The Import AP(s) Tab....40
6.1.3 The Create AP Tab....41
6.2 Monitoring....43
6.2.1 Status Table....44
6.2.2 Pop-up box for an AP....45
6.3 Changing the Settings of an AP....47
6.3.1 General Settings....48
6.3.2 Radio Settings....49
6.3.3 Advanced Settings....52
6.3.4 Hotspot Settings (x)....52
6.4 Saving the Settings of an AP....54
6.5 Applying the Settings to an AP....54
6.6 Changing the Settings of Multiple APs Simultaneously....55
6.7 Mesh....55
6.8 Steps to Set Up a Mesh Network....57
6.8.1 RAP Configuration....57
6.8.2 RRC Configuration....59
6.8.3 MAP Configuration....60
6.8.4 Apply the Settings to the APs....61

Section 7: The [Users] Page....62

Section 8: The [Upgrade] Page....63

8.1 APc Upgrade....63
8.2 Older Method of APc Upgrade for APc....64
8.2.1 Upgrading the APc using WinSCP....64
8.2.2 Updating the APc License using WinSCP....65
8.3 AP Upgrade....66
8.3.1 Place Firmware Image on the APc's FTP Server....66
8.3.2 Enter the settings for the FTP....67
8.3.3 Select the Boards....67
8.3.4 Press the Upgrade Button....67

Section 9: The [Account] Page....68

9.1 Account Settings – Password....68
9.2 Account Settings – Email Address....68

9.3 SNMP Settings....68
9.3.1 APc SNMPv3 Settings....68
9.3.2 AP SNMP Settings....69
9.4 Reset....69

Section 10: The [Hotspot] Page....70

10.1 Office....70
10.1.1 Plan List....70
10.1.2 Account List....71
10.1.3 Plan Import ()....72
10.1.4 Plan Export ()....72
10.1.5 Account Import....73
10.1.6 Account Export....73
10.2 Guest....73
10.3 Prepaid....75
10.4 Postpaid....76
10.5 Report....78
10.6 Possible Setup Scenario of Hotspot with Mesh APs and APc..78

Section 11: Troubleshooting....81

11.1 To Check: No Spaces in any Field....81
11.2 Use ping to Check for Connection....81
11.3 Run AP Command to Check-In Manually....81
11.4 To Create AP with MAC Address of wifi0....82
11.5 To Create AP with Correct Model....82
11.6 The World Map needs an Internet Connection....82
11.7 Reset....82
11.8 Error: ionCube PHP Loader....83
11.9 License File Error....84
11.10 Error: mysql_connect....84
11.11 Problem: [Discovery] Scan is Not Finding the AP....84
11.12 Problem: Custom Map uploaded but cannot display....85
11.13 Error: Device cannot check-in because model settings conflict with device model....85
11.14 Problem: AP cannot check-in....85
11.15 Problem: AP can check-in but the APc cannot get the settings from the AP....86

Section 12: Sending Feedback....88

Section 13: Nagios....89

ChangeLog

This chapter shows the changelog for the Compex AP Controller (.iso or .zip file).

APc Upgrade apc_2015-02-06_r168.zip

1. Import Export Plans (Hotspot Office) with same units, simultaneous logins.

APc Upgrade apc_2015-02-04.zip

1. Import Export APs with Custom Map coordinates.
2. If AP is offline, cannot Apply to AP, will send SNMP information once ping is successful.
3. APc kick user by MAC address.
4. Username is “passwordmode” to use Hotspot in Password Mode.
5. Default scan IP range in [Discovery] page to show as 10.121.11.1/26.
6. Any blank rows in Hotspot Import Account and Import Plan .csv files are skipped.
7. Office Account Send Email to user only shows username and password.
8. Walled garden domain and IP address fields expanded to varchar(800).

APc ISO v1.05 2015-01-09

* This APc .iso file can support WPJ344 boards with AP firmware v1.65_b141119 to v1.70_b150127, and WPJ342 boards with AP firmware v1.68_b150209.

* This APc .iso file is compatible with APc upgrades after 2015-01-09 for example apc_2015-02-06_r168.zip.

1. Auto-refresh rate of [Management] page set to 60 seconds.
2. Modify Check Simultaneous Logins and Check Online Users.
3. Add Idle Timeout field to Import and Export Office Accounts list of fields.
4. xl2tpd memory usage increases over time. Hence need to restart it every 5 minutes.
5. Disable nagios.

APc ISO v1.05 2014-12-26

1. Modify the every1minute script to reduce the size of /var/spool/mail/root.

2. Update /etc/raddb.

3. Update freeradius and dependencies to version 2.1.12-6.el6.

4. Support APc upgrade with any filename, not limited to “apc.zip”.

5. The IP address range of the L2TP server is now 10.121.11.x.

6. Create nagios configuration files indirectly when AP check-in to fix the issue "multiple processes of nagios".

APc ISO v1.05 2014-12-11

1. Added /sbin/keep_radius_alive.sh in every1minute crontab.

2. Check if multiple processes of nagios running at the same time then restart it.

APc ISO v1.05 2014-11-24

1. Upgraded from 32-bit to 64-bit CentOS for the APc operating system.

2. Ability to do APc Upgrade and AP Upgrade.

3. Buttons for “Export AP(s)” and “Import AP(s)”, with new Latitude/Longitude information.

4. Map and Status table in [Management] page refreshes automatically every 15 seconds.

5. APs able to check-in automatically after powering on or when APc powers on.

6. Discovery scan shows current IP address being scanned.

7. Able to set World Map zoom.

8. World Map automatically centered onto latest AP position.

9. Map shows mesh APs with status icons and lines denoting the real-time connections.

10. Email alerts to notify user when AP goes down and when AP comes back up.

11. Solved bug of not being able to get max power setting of 11ac radio.

12. Button for [Initialise users] clears the user log to show only the currently connected users.

13. Default Scan IP Range in [Discovery] page set to 131.168.1.1/26.

14. Improved the fonts for the AP mode/status icons.

15. Initial APc firmware for the Chinese Baidu Maps version.

16. Able to show VAP information for mesh APs when clicking the “+” in the Status table e.g. SSID, Profile, Channel, Encryption, Bit Rate etc.

17. Restart nagios if 2 nagios processes are running.

APc ISO v1.04c 2014-09-15

1. APc version 1.04c with Compex logo, no expiry date.

2. Rebuild xl2tp to fix issue: if-down not execute.

3. Added modules "apc_text apc_uci & apc_restart_service" in snmpd.

4. Modified 'define host' and 'define service' of /etc/nagios/conf.d/*.cfg.

5. Every 1min check & rescue SNMPD.

6. Added plugins for 'localhost' of Nagios.

7. Restart Nagios service when uci check 'l2tpeth.main.restartNagios=1'.

8. First version 64 bits.

9. Fixed issue: 'duplicate users in Hotspot Report' cause by Radius being configured wrongly.

APc ISO v1.04a 2014-08-14

1. Can enable/disable IPsec StrongSwan.

2. Increased Linux upload max file size limit from 2 MB to 10 MB.

3. Added netmask prompt to initial config script (to show in /bin/apc.init.sh script).

APc ISO v1.01 2014-07-25

1. Added device_ip_l2tp in database of APc.

2. AP discovery and check-in using L2TPv3.

3. Beta version with l2tpv3/IPSev Server.

4. Fixed Error: email alert, edited /var/spool/cron/root.

5. Add kernel 2.6.39, l2tpv3tun.

6. After “Create AP”, automatic update of IP in Nagios & database.

7. When clicking “Group Delete/Delete Network/Reset to default” it also updates Nagios List IP.

8. Currently “Delete” button doesn't work.

9. Added '/etc/rc.d/init.d/WatchNagios' to check every 2 seconds: If the config file of Nagios changes then restart Nagios service.

10. Check-in and check-out time can follow time zone other than UTC+0.

APc ISO v1.00 2013-08-01

1. Initial APc firmware.

Section 1: Overview of the AP Controller

The Access Point (AP) Controller, or APc, provides centralized management for CompexWRT APs.

The APc makes use of SNMPv3 protocols to manage and monitor the APs.

1.1 Features

Most of the features available on the configuration web page of the CompexWRT APs are available on the APc. Customers can use our APc to edit an AP individually, or group them together and edit at the same time.

The APc monitors all the virtual APs (VAPs) of each CompexWRT AP to provide the user with a full overview of what is happening on the AP.

1.1.1 Discovery

The APc can scan for connected APs.

SNMPv3 authentication is performed while scanning for connected APs.

1.1.2 Management (Monitoring)

The Google Map or Custom Map allows customers to place their APs.

The APc displays each individual AP's statistics such as the IP address, MAC address, model of the board, and version of the firmware.

The APc also monitors each individual AP's status such as the virtual AP (VAP) status, uptime, time since the last check-in, and free memory.

Each individual VAP's statistics are also displayed. These include the MAC address, SSID, channel, encryption, and bit rate.

The APc monitors end users (e.g. mobile phone, laptop) connected to the AP as well as CompexWRT stations connected to the AP. The parameters shown include the hostname, IP address, MAC address and SSID that it is connected to. The TX rate, RX rate, and TX CCQ are also included. The list of end users are updated every 15 seconds, while the Stations are updated every 1 minute.

1.1.3 Management (Changing the Settings of Devices)

The settings for each individual radio can be modified.

Up to 16 SSIDs/VAPs can be created for each radio.

The wireless profile, channel, transmit power, and ACK-TimeOut value can be viewed and edited.

You can also change the settings for individual SSIDs, such as the wireless mode, encryption, MAC filter, etc.

The “Group Edit” button allows you to apply settings for multiple selected APs at the same time.

1.1.4 Users

The APc keeps a record of end users (e.g. mobile phone, laptop) connected to all the APs. The parameters shown include the hostname, IP address, MAC address and SSID that it is connected to. The upload data usage, download data usage are also shown. The end users are updated every 15 seconds.

You can view the log of all the users up to 5 days. The MAC Address, check-in time and check-out time are shown.

1.1.5 Firmware Upgrade

The APc lets you upgrade multiple selected APs concurrently.

The SNMPv3 is used to manage the upgrade process.

The FTP protocol is used to transfer the firmware image.

The status is also updated to the APc (successful or unsuccessful).

1.1.6 Nagios based monitoring

The APc makes use of Nagios for monitoring the APs.

Nagios is an open-source network management system.

Customers can customize any other types of status to be monitored.

An alert plugin can be used for sending SMS.

There is also support from the community.

More information about Nagios can be read on http://www.nagios.org/

1.2 Hardware and Software Components

The APc resides in a small and lightweight hardware. The APc comes pre-installed, tested, and pre-configured for use.

Alternatively, the APc may be installed on a virtual machine, using an 'iso' file.

The APc runs Nagios on Centos.

Nagios is an open source computer system monitoring, network monitoring, and infrastructure monitoring software application. Nagios offers monitoring and alerting services for servers, switches, applications, and services. It alerts the users when things go wrong and alerts them a second time when the problem has been resolved.

CentOS (abbreviated from Community Enterprise Operating System) is a Linux distribution that attempts to provide a free enterprise class computing platform which has 100% binary compatibility with its upstream source, Red Hat Enterprise Linux.

The CompexWRT APs make use of CoovaChilli to offer the Hotspot functionality.

CoovaChilli is an open-source software access controller, based on the popular (but now defunct) ChilliSpot project. CoovaChilli is a feature rich software access controller that provides a captive portal / walled-garden environment and uses RADIUS or a HTTP protocol for access provisioning and accounting.

A RADIUS server resides in the APc.

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service.

1.3 Licensing

The 'iso' file for the APc would be available on our website.

The customer is to fill up a form to send an enquiry to us. We would send them by email a 2 weeks evaluation license. Note: the license starts from the day Compex creates the license, not when the customer starts using the files. After 2 weeks, they can buy a license for up to 1 year of usage, with email support.

1.4 Layout of this Manual

The sections in this manual correspond closely to the vertical menu bar in the configuration web page of the APc. The vertical menu bar provides the links to the following pages:

- [Discovery]
- [Create Network]
- [Network]
- [Management]
- [Users]
- [Upgrade]
- [Account]
- [Hotspot]
- [Documentation]
- [Feedback]

Section 2: Getting Started with the APc

Section 2.2 *Installing the .iso File to a PC – Initial Step* describes the installation of the APc on a PC. If installing the APc on a virtual machine, you may jump to Section 2.3 *Installing the .iso File on a Virtual Machine – Initial Step*.

Next, Section 2.4 *Installing the .iso File – Subsequent Steps* is to be followed.

Section 2.5 *Perform Initialization by Running Three Scripts* explains how you can perform initialization by running three commands.

If the APc comes as a pre-installed hardware, you may connect the hardware to the network and jump to Section 2.6 *Logging in to the APc*.

2.1 Download the .iso File

First download the .iso file and save it to a temporary folder e.g. “C:\Temp\”

The .iso file available from our website is a virtual optical disk file that can be used to install the operating system of the APc.

Say for example the .iso file is called “APc_0904.iso”.

2.2 Installing the .iso File to a PC – Initial Step

2.2.1 Using a DVD Optical Drive to Install on a PC

The easiest way is to create a DVD installation boot disk using a CD/DVD writing software such as CDBurnerXP. Please burn the .iso image file to a DVD.

Attach an external DVD drive to the PC that would function as the APc, using USB cables.

Reboot the PC. You may have to press “F12” to enter the boot menu.

Choose to boot up using the DVD.

2.2.2 Using a USB Flash Drive to Install on a PC

This method is more complicated than using a DVD but it would save the cost of one DVD, and would not require an external DVD drive.

You would need a USB flash drive with at least 2 GB capacity.

You would also need the UNetBootin open source software (Universal Netboot Installer).

Please format your flash drive to use the FAT32 file system. (FAT may also be permitted.)

After that, please run the UNetBootin software.

Please select: Diskimage: ISO, and browse for the .iso file.

Please select: Type: USB Drive, and choose the correct drive letter.

Next, press “OK”.

When asked to overwrite files, please select “Yes to All”.

It may take 5 minutes to copy all the files to the flash drive.

When asked if you want to reboot now, don't click “Reboot Now”. Instead, click “Exit” because you are installing the APc into a different PC.

Next, copy the .iso file itself into the root directory of the flash drive. The filename does not matter, as long as it has the .iso extension. This is to prevent the following error later: “Missing ISO 9660 image: The installer has tried to mount image #1, but cannot find it on the hard drive”

Safely eject this flash drive, then insert it into the PC that would function as the APc.

Reboot the PC. You may have to press “F12” to enter the boot menu.

Choose to boot up using the flash drive.

Installation Method

What type of media contains the installation image?

- Local CD/DVD
- **Hard drive**
- NFS directory
- URL

Please choose “Hard drive”.

Select Partition

What partition and directory on that partition holds the installation image for CentOS? If you don't see the disk drive you are using listed here, press F2 to configure additional devices.

- /dev/sda1
- /dev/sda2
- /dev/sdb1

(Directory holding image)

There is a bit of trial and error here. Please try one by one. If an error message pops up, click “OK” and try the next one. One of them is the correct one and then you can proceed.

2.3 Installing the .iso File on a Virtual Machine – Initial Step

This section describes the installation of the APc on a virtual machine (VM) using a virtualization software such as VirtualBox. VirtualBox is used for this example.

2.3.1 Create the VM

Create the VM with the following options.

Name and operating system

- Name: APC1 (for example)
- Type: Linux
- Version: Ubuntu (64 bit)

Memory size

- Random access memory (RAM) size: 645 MB

Hard drive

- Create a virtual hard drive now:
- Hard drive file type: VDI (VirtualBox Disk Image)
- Storage on physical hard drive: Dynamically allocated
- File location: “C:\VMs\APC1\APC1.vdi” (for example)
- File size: 8 GB

2.3.2 Settings for the VM

Once the VM is created, make sure you have the following settings.

- System > Processor > Extended Features > Enable PAE/NX
  - PAE/NX stands for “Physical Address Extension / no execute”.
- Network > Enable Network Adapter > Bridged Adapter:
  - Select the adapter that is used for obtaining network access.

2.3.3 Note for VMware

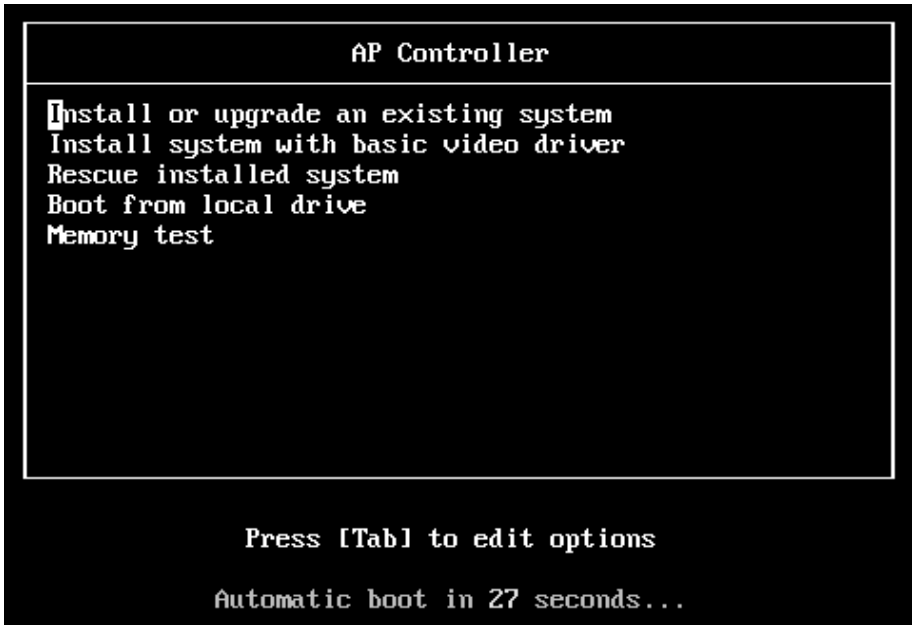
For VMware, it has been found that a new network card must be added in the VM hardware setting so that the eth0 can be discovered. The network script would then be able to run properly.

2.4 Installing the .iso File – Subsequent Steps

Boot the computer (or VM) using this .iso file.

A black screen is displayed with the following text:

- AP Controller
  - Install or upgrade an existing system
  - Install system with basic video driver
  - Rescue installed system
  - Boot from local drive
  - Memory test
- Press [Tab] to edit options
- Automatic boot in 59 seconds...


AP Controller
Install or upgrade an existing system
Install system with basic video driver
Rescue installed system
Boot from local drive
Memory test
Press [Tab] to edit options
Automatic boot in 27 seconds...

Simply press [Enter] or select the first option “Install or upgrade an existing system”.

Next, a grey dialog box over a blue background appears, with the following text.

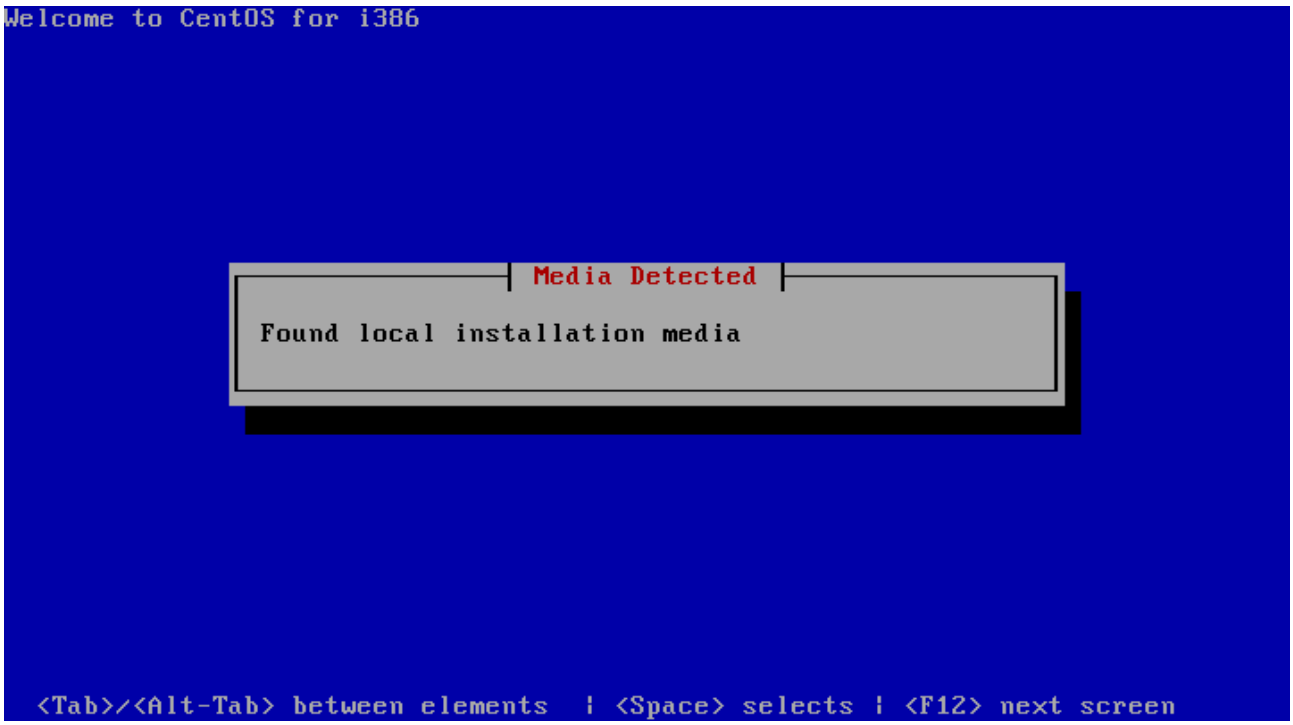
- Disk Found
  - To begin testing the media before installation press OK.
  - Choose Skip to skip the media test and start the installation.
  - OK Skip

Note: Please choose “Skip”.

- This is important because the .iso file is not a standard Linux distribution release and has a different checksum.
- Choosing “OK” has been found to corrupt the VM. The installation would have to be started again from the beginning.

After clicking “Skip”, a message appears:

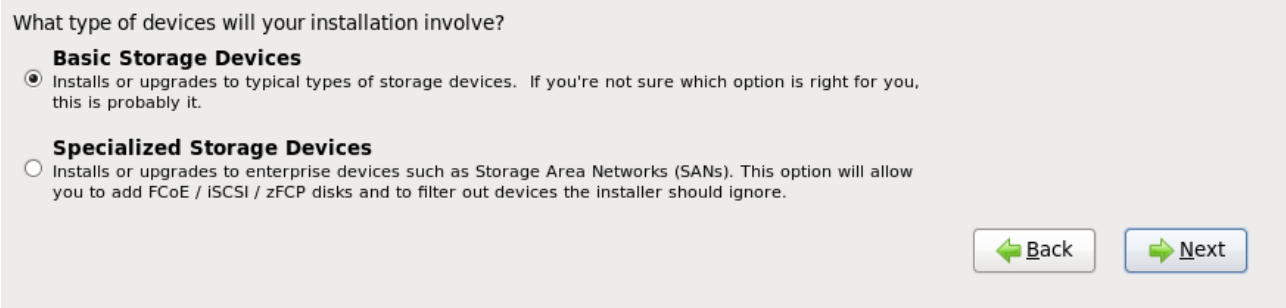
- Media Detected
  - Found local installation media



Next, the Compex splash screen appears.

Click Next. Continue through the following screens.

- What language would you like to use during the installation process?:
  - English (English).
- Select the appropriate keyboard for the system:
  - e.g. U.S. English.
- What type of device would your installation involve?:
  - Basic Storage Devices

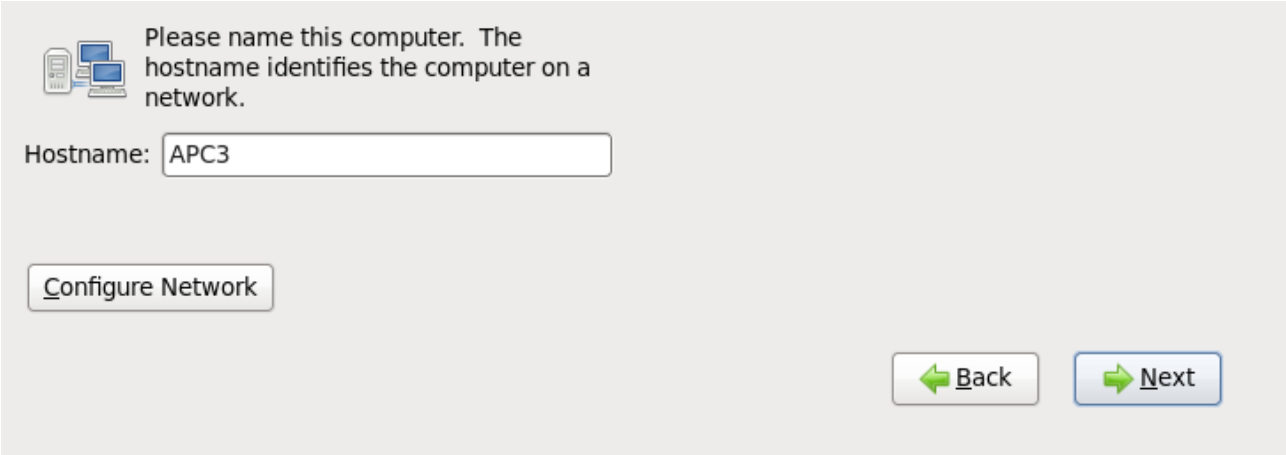

What type of devices will your installation involve?
Basic Storage Devices
Installs or upgrades to typical types of storage devices. If you're not sure which option is right for you, this is probably it.
Specialized Storage Devices
Installs or upgrades to enterprise devices such as Storage Area Networks (SANs). This option will allow you to add FCoE / iSCSI / zFCP disks and to filter out devices the installer should ignore.
Back
Next

- Storage Device Warning: The storage device below may contain data:
  - Click the appropriate button:
    - Yes, discard any data.
    - No, keep any data.
  - For a new disk, the choice does not matter.

Storage Device Warning
The storage device below may contain data.
ATA VBOX HARDDISK
8192.0 MB pci-0000:00:0d.0-scsi-0:0:0:0
We could not detect partitions or filesystems on this device.
This could be because the device is blank, unpartitioned, or virtual. If not, there may be data on the device that can not be recovered if you use it in this installation. We can remove the device from this installation to protect the data.
Are you sure this device does not contain valuable data?
Apply my choice to all devices with undetected partitions or filesystems
Yes, discard any data
No, keep any data
Back
Next

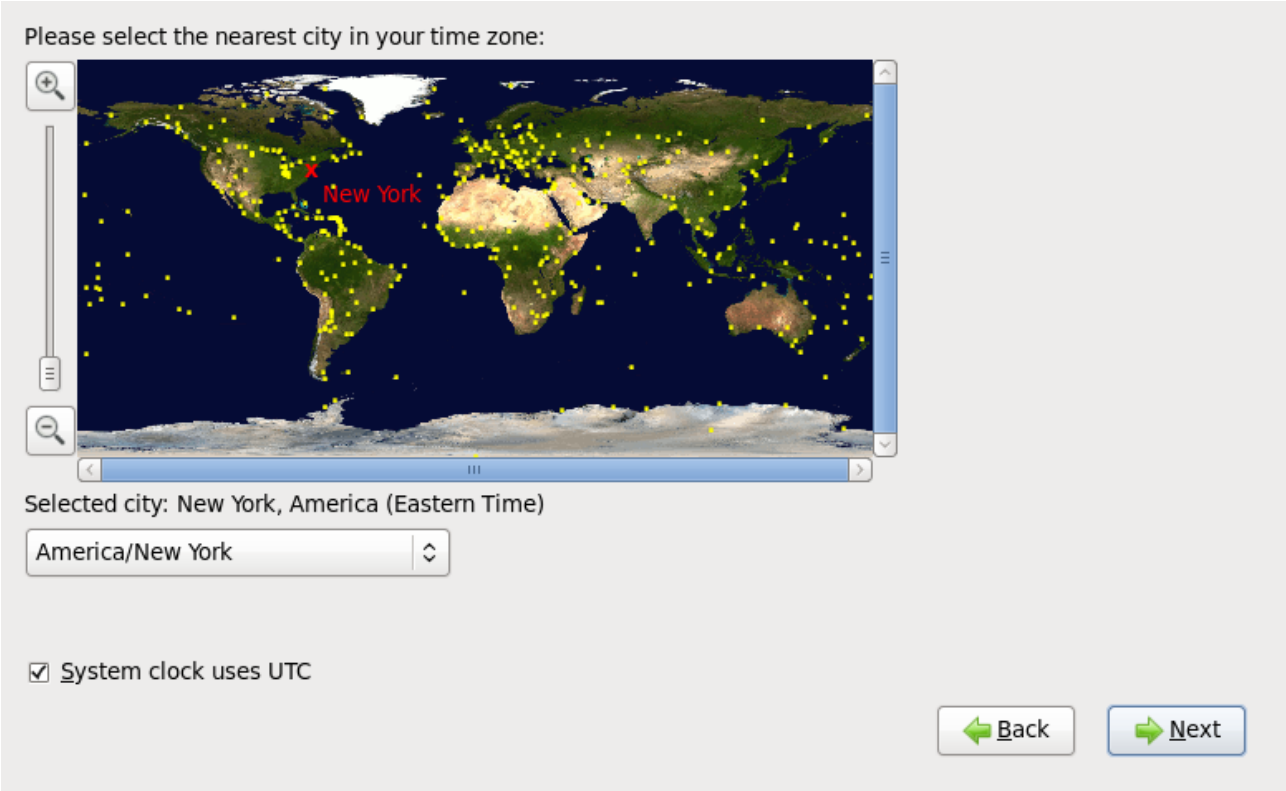
Please name this computer. The hostname identifies the computer on a network.

- Hostname: APC1 (for example).
- Do not click on “Configure Network”.



Please select the nearest city in your timezone.

- System clock uses UTC: You may leave this option checked.

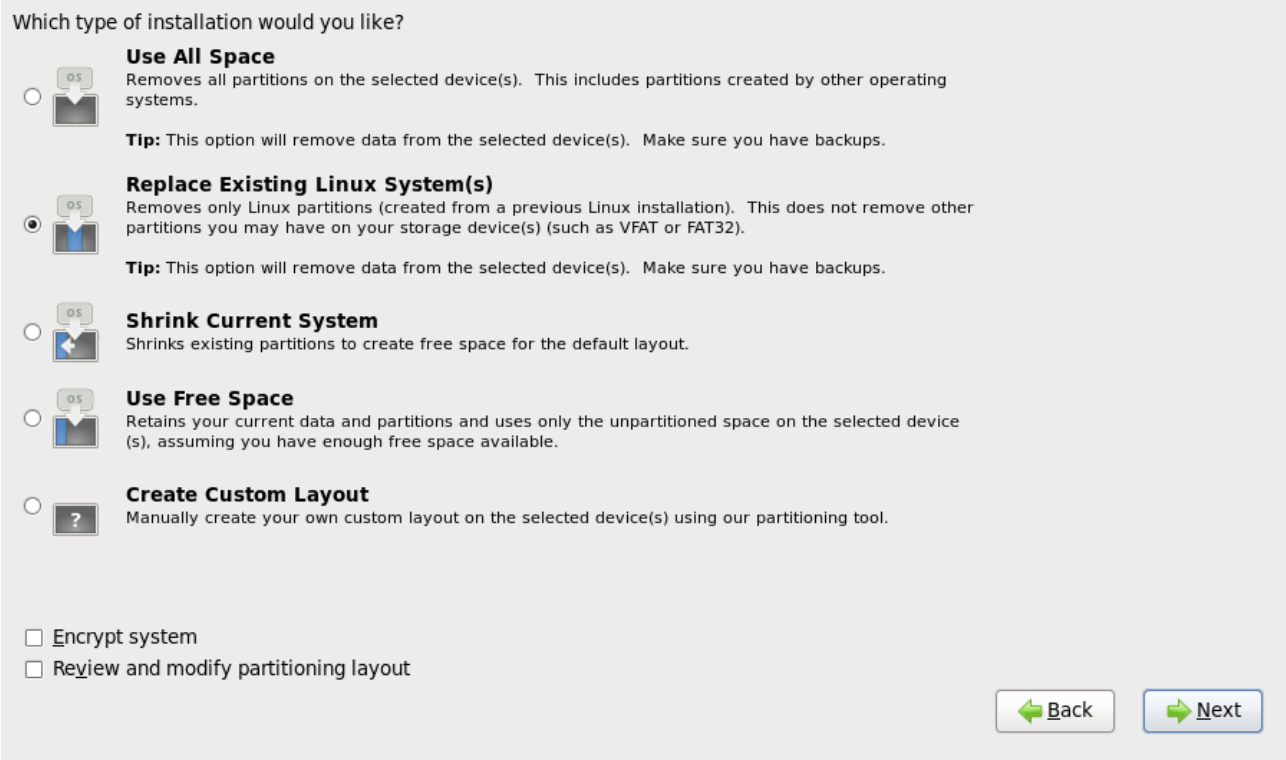


The root account is used for administering the system. Enter a password for the root user.

- You may select your own password, e.g. “root_password”.

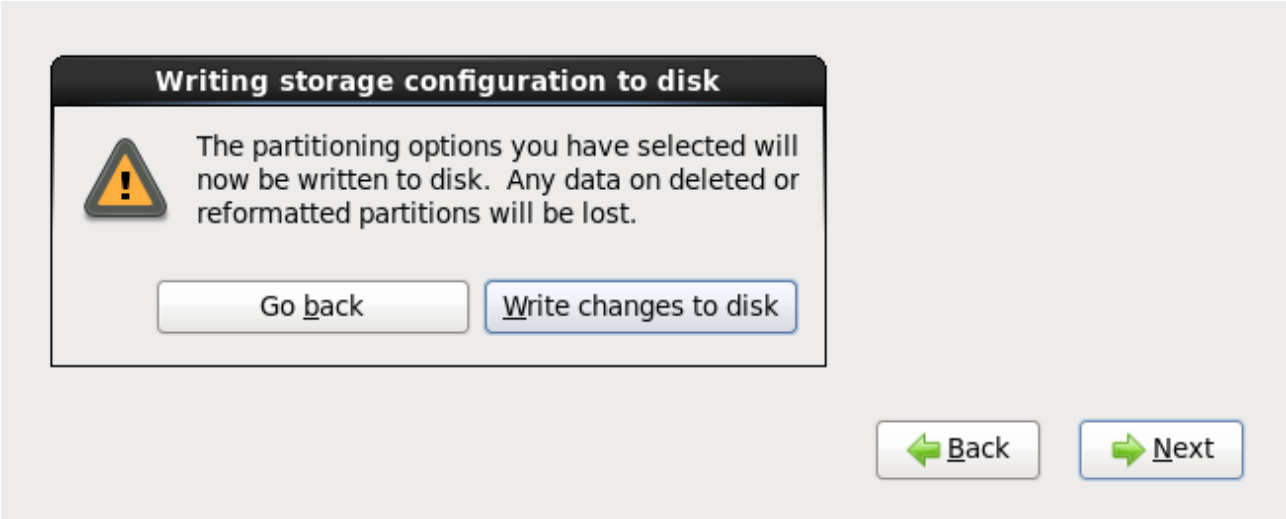
Which type of installation would you like?

- Replace Existing Linux System(s).


Which type of installation would you like?
Use All Space
Removes all partitions on the selected device(s). This includes partitions created by other operating systems.
Tip: This option will remove data from the selected device(s). Make sure you have backups.
Replace Existing Linux System(s)
Removes only Linux partitions (created from a previous Linux installation). This does not remove other partitions you may have on your storage device(s) (such as VFAT or FAT32).
Tip: This option will remove data from the selected device(s). Make sure you have backups.
Shrink Current System
Shrinks existing partitions to create free space for the default layout.
Use Free Space
Retains your current data and partitions and uses only the unpartitioned space on the selected device (s), assuming you have enough free space available.
Create Custom Layout
Manually create your own custom layout on the selected device(s) using our partitioning tool.
Encrypt system
Review and modify partitioning layout
Back
Next

Writing storage configuration to disk:

- Write changes to disk.


Writing storage configuration to disk
The partitioning options you have selected will now be written to disk. Any data on deleted or reformatted partitions will be lost.
Go back
Write changes to disk
Back
Next

The installation process would start. It may take a few minutes to complete the installation. Once completed, the following message is displayed.

- Congratulations, your CentOS installation is complete.
- Please reboot to use the installed system. Note that updates may be available to ensure the proper functioning of your system and installation of these updates is recommended after the reboot.

Click the “Reboot” button.

After the reboot, the terminal shows:

- APC1 Login:
  - Please enter “root” as the username.
  - The password is the same as the one chosen earlier, e.g. “root_password”.

You would then come to the Linux command prompt (terminal).

2.5 Perform Initialization by Running Three Scripts

There are three commands that you would have to run to initialize the APc:

- **`/bin/apc.init.sh`**
- **`/bin/mysql.init.sh`** (not required for APc v1.03 onwards)
- **`/bin/ftp.init.sh`**

Each command calls a specific shell script.

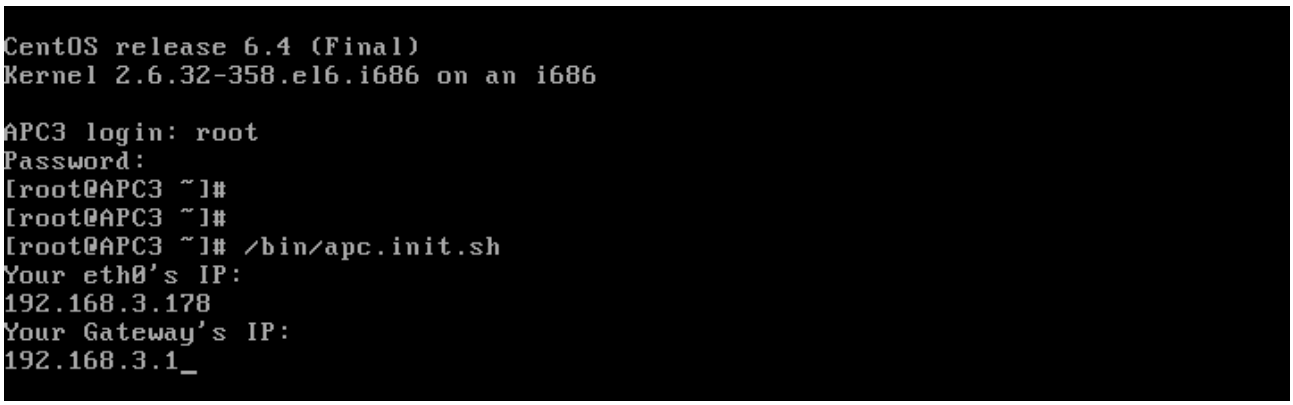
2.5.1 Run the Script for 'apc'

In the Linux terminal, enter the following command to configure the network:

- **`/bin/apc.init.sh`**

Please input the following fields:

- Your eth0's IP:
  - Enter the static IP address that the APc would have on the network, e.g. 192.168.3.178
- Your Gateway's IP:
  - e.g. 192.168.3.1
- Your Subnet Mask:
  - e.g. 255.255.255.0



The system would do some processing and then reboot.

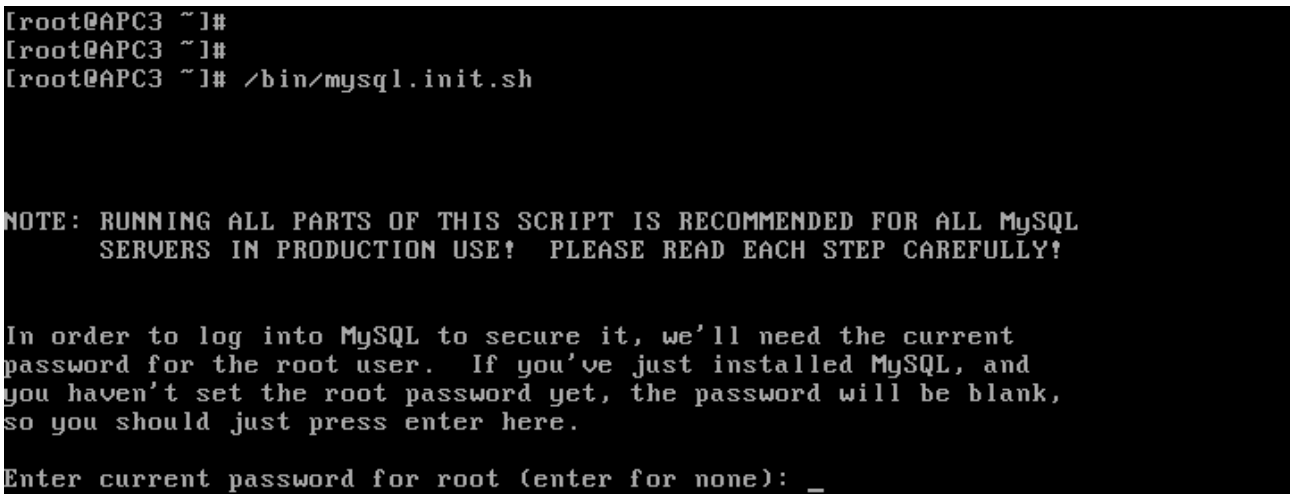
2.5.2 Run the Script for 'mysql'

This script is not required for the APc v1.03 onwards, because it is automatically run in the script for 'apc' already.

In the Linux terminal, enter the following command to configure the database:

- **/bin/mysql.init.sh**

Enter current password for root (enter for none): Please just press the “Enter” button.


[root@APC3 ~]#
[root@APC3 ~]#
[root@APC3 ~]# /bin/mysql.init.sh
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!
In order to log into MySQL to secure it, we'll need the current
password for the root user. If you've just installed MySQL, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.
Enter current password for root (enter for none): _

Set root password? Yes.

New password:

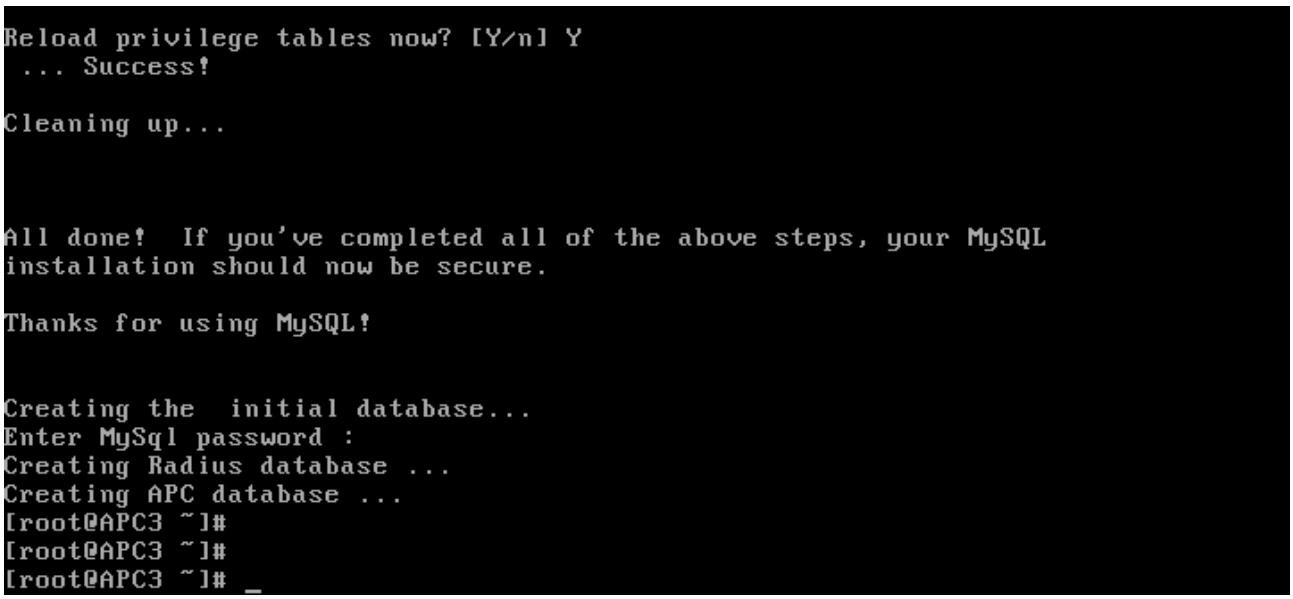
- Please use this password: apc0ntr0ll3r
- Notice the digits 0,0,3.

```
Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MySQL
root user without the proper authorisation.

Set root password? [Y/n] Y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MySQL installation has an anonymous user, allowing anyone
to log into MySQL without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] Y_
```

Following that, there are a series of questions. Please enter the default option “Y” for “Yes” at each prompt.

```
Remove anonymous users? [Y/n] Y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] Y
 ... Success!

By default, MySQL comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] Y
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] Y_
```

More question prompts. Enter the default “Y”.


Reload privilege tables now? [Y/n] Y
... Success!
Cleaning up...
All done! If you've completed all of the above steps, your MySQL
installation should now be secure.
Thanks for using MySQL!
Creating the initial database...
Enter MySql password :
Creating Radius database ...
Creating APC database ...
[root@APC3 ~]#
[root@APC3 ~]#
[root@APC3 ~]# _

Enter MySql password:

- Please use this same password: apc0ntr0ll3r
- Notice the digits 0,0,3.

2.5.3 Run the Script for 'ftp'

Any FTP server can be used for the AP firmware upgrade capability. The following describes the procedure if you wish to install an FTP server inside the APc itself.

In the Linux terminal, enter the following command:

- **`/bin/ftp.init.sh`**

Creating username and password for FTP server:

- Type username: ftpuser (for example)

Changing password for user ftpuser:

- New password: ftppass (for example)

```
[root@APC3 ~]#
[root@APC3 ~]#
[root@APC3 ~]# /bin/ftp.init.sh
Creating Username & password for FTP server
Type username:
ftpuser
Changing password for user ftpuser.
New password:

Retype new password:
passwd: all authentication tokens updated successfully.
[root@APC3 ~]#
[root@APC3 ~]#
[root@APC3 ~]# _
```

Once the username and password are created, a new folder is created in the /home directory:

- /home/ftpuser/ (for example)

Later in Section 8.3 *AP Upgrade*, the process of upgrading the firmware of APs using the [Upgrade] page is explained.

2.6 Logging in to the APc

On your computer, you may use an Internet browser to access the APc's configuration web page. While any browser can be used, the Firefox browser is preferred due to its low memory usage.

The URL of the APc is the IP address of the APc followed by /apc/, for example:

- http://192.168.3.178/apc/

The default login information for the APc is:

- Username: admin
- Password: password

Figure 1: The Login page

The “Registration” button is for the creation of the account for the AP Controller. For each APc, there is only one account.

When logging in for the first time, you have to create an APc network, which organizes the CompexWRT APs. The section on “Creating an APc Network” describes this process.

Multiple concurrent logins are not allowed. This is to prevent any conflict that may occur when two persons change a particular AP's settings at the same time.

If there is an existing login, and another login is performed, the earlier instance would be logged out with the error message: “You are logged in at another place.”

Section 3: Creating an APc Network on the [Create Network] Page

When using the APc for the first time, a message would appear: “There is no network in your account. Please create one first.”

In the [Create Network] page, you can create a new APc network. The APc allows you to organize the connected APs into APc networks. You could have one APc network that controls all the APs or have multiple APc networks that control different APs. An AP can come under only one APc network.

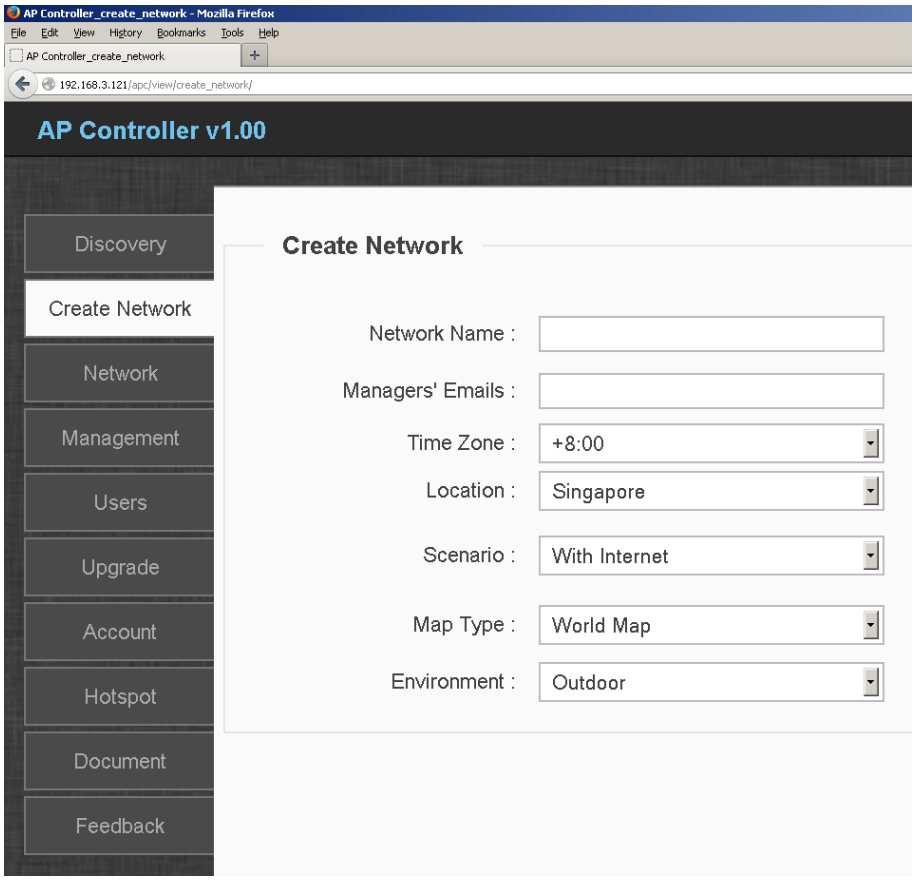


Figure 2: The [Create Network] page.

Note: You may not use any of the following characters in any of the textbox fields in the APc web page:

- space “ ”
- ampersand “&”
- plus “+”
- double quote “"”

- single quote “'”
- backslash “\”

If you clicked the “Save Settings” button, a warning message would pop up if the text is not accepted e.g. “Please input correct username.”

The reason is that these characters are used for the Linux, SNMP, and PHP commands.

The fields in the [Create Network] page are explained as follows.

Network Name: This is the name for your network. Every network should have their own unique name. Each AP can only exist in one APc network.

Managers' Emails: This is the default email address that the APc would send email to if an AP goes down or comes back up. You can add multiple email addresses and separate them by comma(,) without spaces. For example: email1@gmail.com,email2@gmail.com

Time Zone: Please select the time zone you are in.

Location: Please select the country you are in.

Note: “Location” has no relation with the “Country” setting on the APs. The map of this country would be displayed in the [Management] page, when the Google Map is used.

Scenario: If the MeshPoints are used to provide Internet coverage, choose “With Internet”. If the MeshPoints are used to provide connectivity in a closed environment, without access to the Internet, choose “No Internet”.

Note: If you choose “With Internet” option when there is no internet, there might be problems such as the inability to show the Google map later. A reset to default settings in the [Account] page may be required.

Map Type: “World Map” utilizes the Google Map for you to put the MeshPoints on, whereas “Custom Map” allows you to upload an office/any other layout.

If you had chosen “No Internet” for the *Scenario* option, the *Map Type* would be set to “Custom Map”.

Environment: Indoor/Outdoor (Outdoor as Default). Select the environment you are in. We enabled higher ACK timeout for Outdoor settings, and thus performance for Indoor devices would be impaired if you use Outdoor settings.

Section 4: APc Network Settings in the [Network] Page

The [Network] page is where you can configure each APc network. The APc network is selectable at the top right corner of the page.

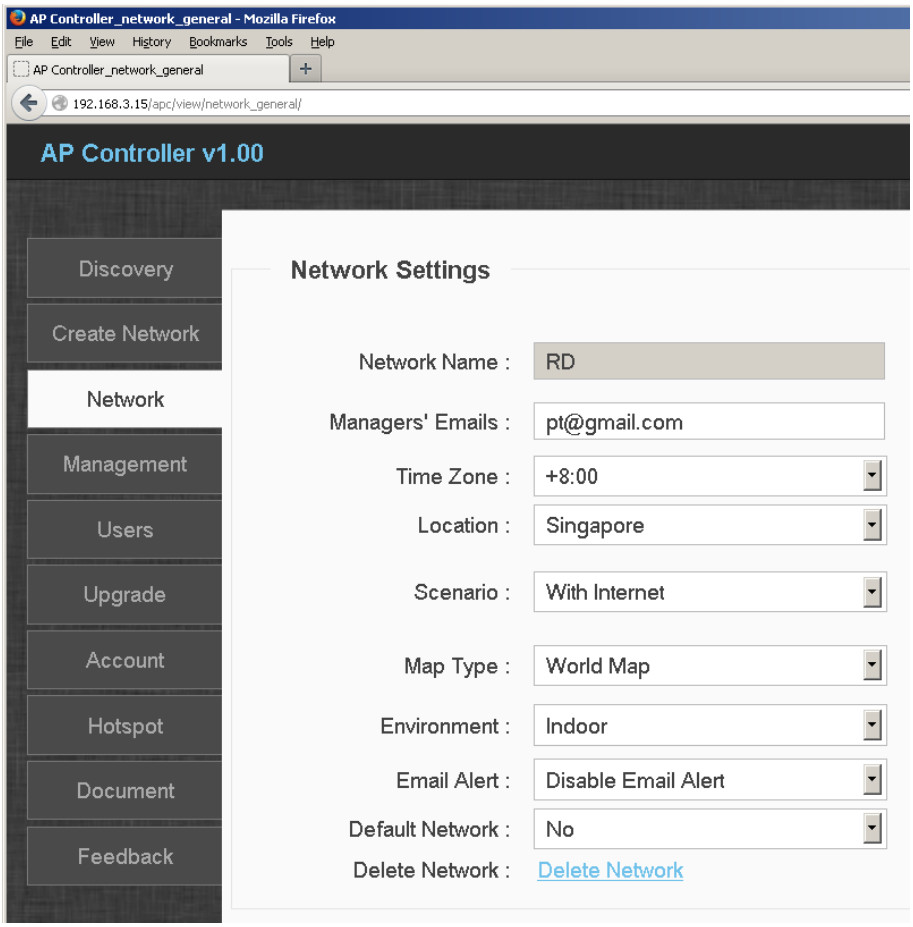


Figure 3: The [Network] page.

The options are the same as in the [Create Network] page. Some additional options are described as follows.

Email Alert: When enabled, messages would be sent to the email addresses specified in "Manager's Emails" whenever an AP goes down or comes back up.

Default Network: Sets this APc network as the default network to be shown when you log in to the AP Controller.

Delete Network: Deletes this APc network and all its settings.

Section 5: Adding APs and using the [Discovery] Page

The AP Controller (APc) can discover CompexWRT APs that are connected. SNMPv3 authentication is used for the scanning of the connected APs.

Suppose that you have APs in your internal LAN networks and the APc resides in the external WAN network. The APc is able to discover and manage them as well.

In this section, the process of configuring the APs and adding the APs using the [Discovery] page is described.

5.1 Configuring the APs

After flashing a new firmware into the AP, or after a reset to factory default settings, please set the IP address of the AP or set the “Protocol” as “DHCP Client”. This is inside the Network > Interfaces > LAN page. After this, please click “Save & Apply”.

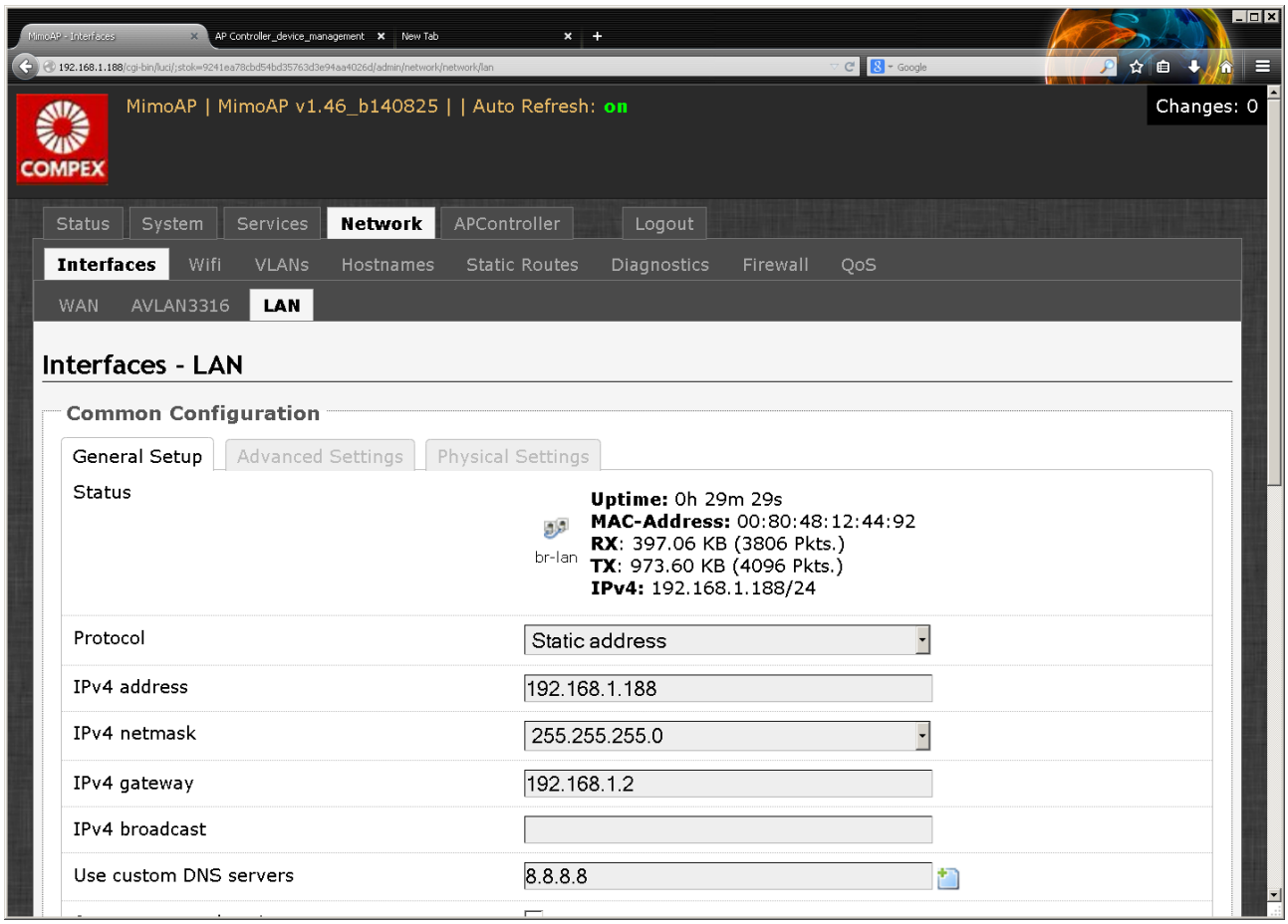


Figure 4: Setting the IP address of the AP.

Next, please go to the APController tab and set the IP address of the APc in the “Remote Server” field.

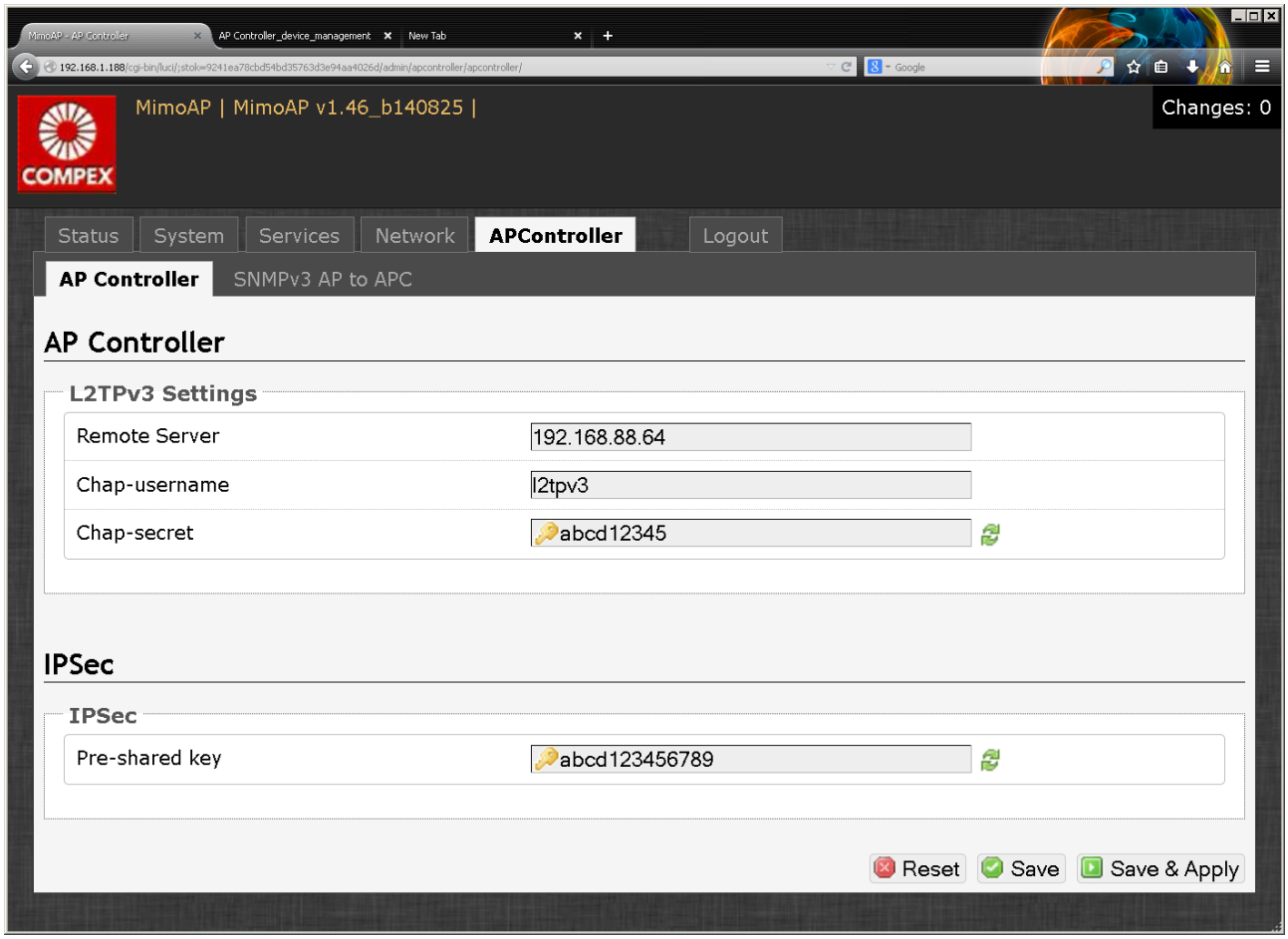


Figure 5: The APController tab in the AP's LuCI web page.

The other settings should be kept as the default for now. Please click “Save & Apply”.

Following that, please click on the Network > Interfaces tab.

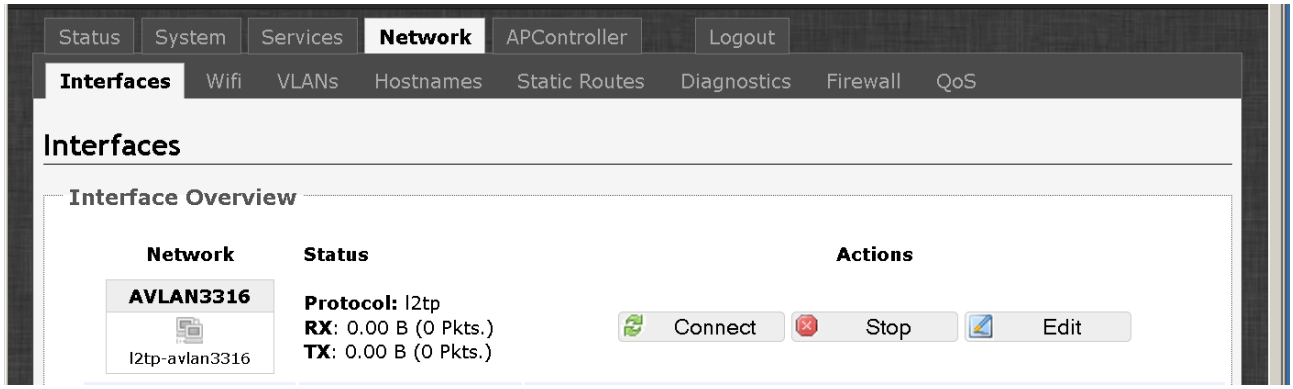


Figure 6: The Network > Interfaces tab of the AP.

The “AVLAN3316” interface is for the L2TPv3 tunnel towards the APc. If there are zero packets received or transmitted, it means that the L2TP tunnel is not working yet.

In a few seconds, you should see that some packets are being communicated via this interface.

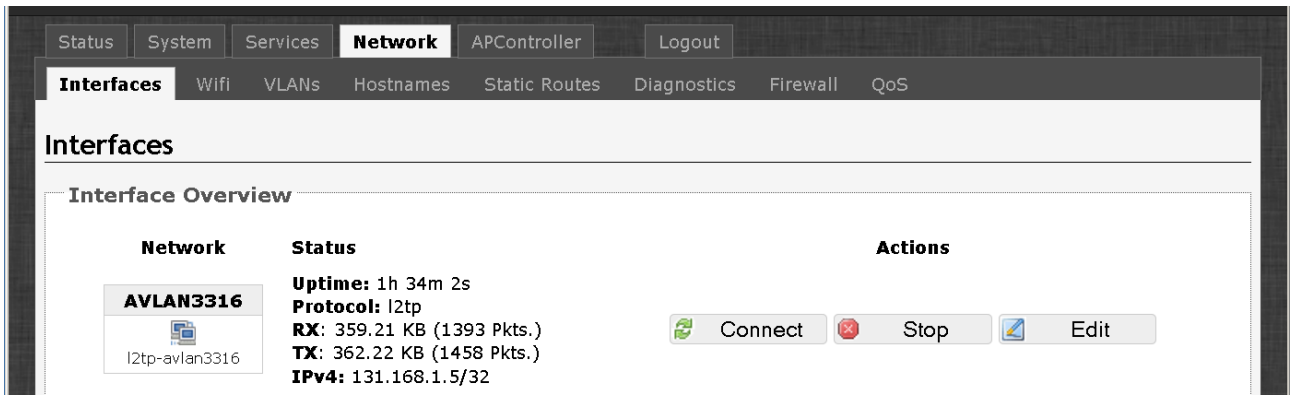


Figure 7: Some packets are being transferred inside the L2TP tunnel.

This means that the L2TP tunnel is established between the AP and the APc. The APc would then be able to discover and add the AP.

Please do not click any of the three buttons inside the Actions section: “Connect”, “Stop”, and “Edit”. This is because the whole process is automatic.

5.1.1 Troubleshooting Steps if the L2TP Tunnel is Not Working

Please click “Save & Apply” in the APController tab. Then go to the “Network” tab to check the status of the L2TP tunnel again.

The following is another way to check the status of the L2TP tunnel.

Login to the AP's shell and enter this command:

- **`ifconfig`**

If you see an entry for “l2tp-avlan3316”, this means that the L2TP is running on the AP:

```
l2tp-avlan3316 Link encap:Point-to-Point Protocol
          inet addr:131.168.1.6  P-t-P:131.168.1.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1410  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:729 (729.0 B)  TX bytes:674 (674.0 B)
```

Otherwise, the L2TP is not running on the AP.

You may also run this command:

- **`while true; do sleep 2; uci show apc.setting.1minuteUd; done`**

Do you see something like this:

```
...
apc.setting.1minuteUd=0
apc.setting.1minuteUd=0
```

```
apc.setting.1minuteUd=0
apc.setting.1minuteUd=1
apc.setting.1minuteUd=1
apc.setting.1minuteUd=0
apc.setting.1minuteUd=0
apc.setting.1minuteUd=0
...
```

You should see the line “apc.setting.1minuteUd=1” appear every one minute because the AP attempts to update the APc every sixty seconds. This would show that the L2TP is running on the AP. If the L2TP is not running, please reboot the AP:

- **`reboot`**

If the L2TP tunnel is still not working, login to the APc's shell and run this command:

- **`service xl2tpd restart`**

If these methods do not work, manually power off the AP, wait 10 seconds, and power on again. It was found that this is the best method to get the L2TP tunnel to start.

Once you see that the L2TP tunnel is communicating packets, you can go to the APc web page to discover and add the APs.

5.2 Adding APs

This section describes the process of adding APs to the APc network.

There are a few ways to add APs:

- Using the [Discovery] page.
- Using the “Import AP(s)” tab on the [Management] page.
- Using the “Create AP” tab on the [Management] page.

The “Import AP(s)” and “Create AP” tabs allow you to add APs to the APc network even before they are connected. This would be useful for system integrators as it may simplify the process of adding a multiple number of new APs. More information can be found in Section 6.1.2 *The Import AP(s) Tab* and Section 6.1.3 *The Create AP Tab*.

The following section describes the use of the [Discovery] page.

5.3 Using the [Discovery] Page to add APs

The first page in the APc web page is the [Discovery] page. This is where you can perform the scan for a selected network. The network is selectable at the top right corner of the page.

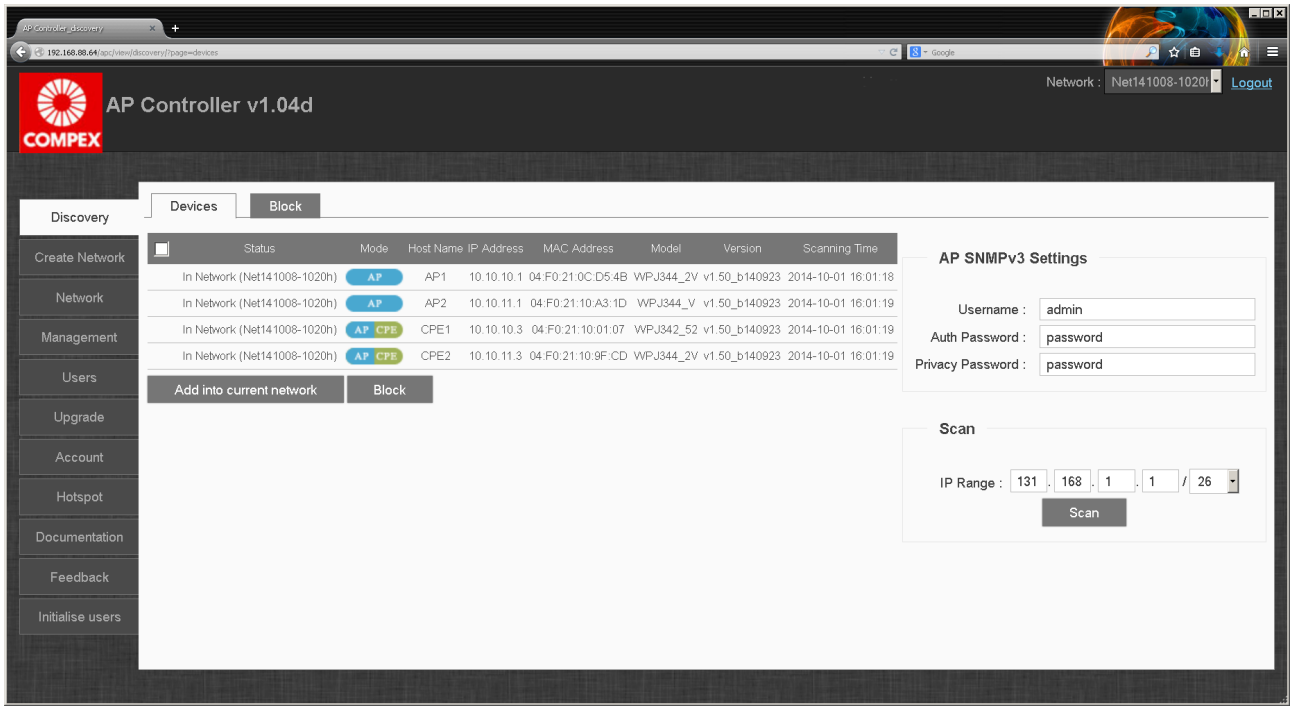


Figure 8: The [Discovery] page of the APc.

5.3.1 AP SNMPv3 Settings

Looking at the right side of the page, the parameters for SNMP can be set.

The APc and AP use the SNMPv3 authentication. The default values for the AP SNMP settings are given in Section 9.3.2 AP SNMP Settings.

5.3.2 Scan IP Range

For the APc v1.04a and above, please set the IP Range for the Scan in the APc's [Discovery] page as:

- 131.168.1.1/26

The reason is that the L2TPv3 tunnel is now connecting the APc to the APs. The AP firmware version should also be version b140814 and above.

For the APc v1.05_b141226 and above, please set the IP Range for the Scan as:

- 10.121.11.1/26

The AP firmware version should also be version b141128 and above.

This procedure also works if some of the APs are in the same subnet as the APc.

As long as the AP can ping to the APc, the APc would be able to discover it.

Another advantage of using the APc v1.04a and above is that the scanning time is much reduced. This is because the L2TPv3 tunnel IP addresses assigned by the DHCP server start from a small number: 131.168.1.1.

5.3.3 Note on the Scanning Time

Suppose the Scan IP Range is set as 131.168.1.1/26. This means that all APs in the 131.168.1.1/26 network would be scanned. The scan takes about 2 seconds per IP address. For this example, since the network is determined by the first 26 bits of the IP address, there are about 2^(32 – 26) = 2^(6) = 64 IP addresses to be scanned. Therefore the scanning time would be about 2 minutes.

Figure 9: Now scanning -> current IP address.

While the scanning is in progress, newly discovered APs are listed in real-time. If all the new APs are seen to be discovered already, the scan can be stopped by clicking the “Stop scanning” button.

5.3.4 The Devices Table

Once the scan is completed, the APs discovered would be listed in the table under the “Devices” tab. This Devices table shows the APc network where the AP is in. APs that have not been added to any APc network would show up with the Status as “New”.

You can add the AP into the current APc network by clicking the button “Add into current network”. You may block the AP so that it cannot be added to this APc network the next time the scan is performed. This can be done by clicking the “Block” button. Note that AP has to be selected first by ticking the checkbox, before clicking the button that performs the action.

If the AP had already been added to any APc network, the checkbox beside it disappears. Instead of “New”, the Status shows the name of the APc network that the AP is in. For example “In Network (PT)” means that the AP is in the APc network called “PT”.

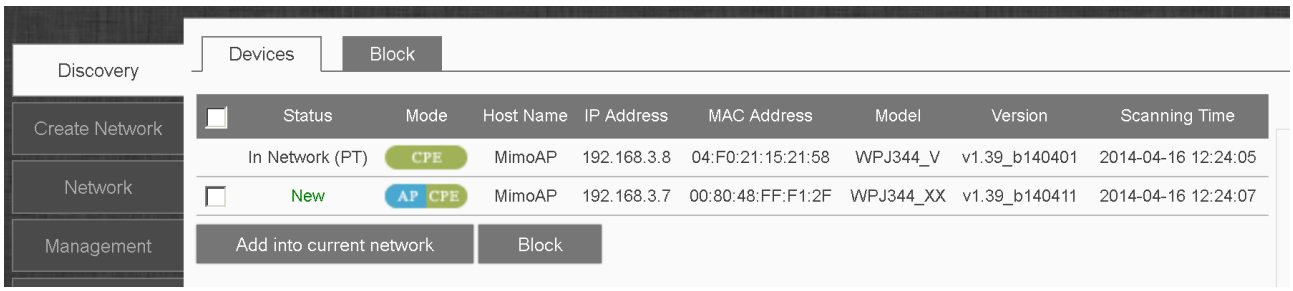


Figure 10: Table under the “Devices” tab of the [Discovery] page.

To block an existing AP, first go to the [Management] page to delete the AP, then return to the [Discovery] page to block it.

5.3.5 The Mode / Status icon

The Mode / Status icon of an AP is determined by the first VAP of the radio(s).

If an AP has one radio, the radio could have the first VAP configured as AP mode or Station mode. The mode icon would show “AP” for AP mode or “CPE” for Station mode, respectively.

If an AP has two radios, there are a number of configurations that the AP can have. Both radios could have the first VAP configured as AP mode, and the mode icon would show “AP”. Both radios could have the first VAP configured as Station mode, and the mode icon would show “CPE”. Another configuration has one radio with the first VAP configured as AP mode and the other radio with the first VAP configured as Station mode. In this case, the mode icon for the AP would show “AP | CPE”.

Section 6: The [Management] Page

The [Management] page contains a map showing the APs under the selected APc network, as well as a table of the APs' details.

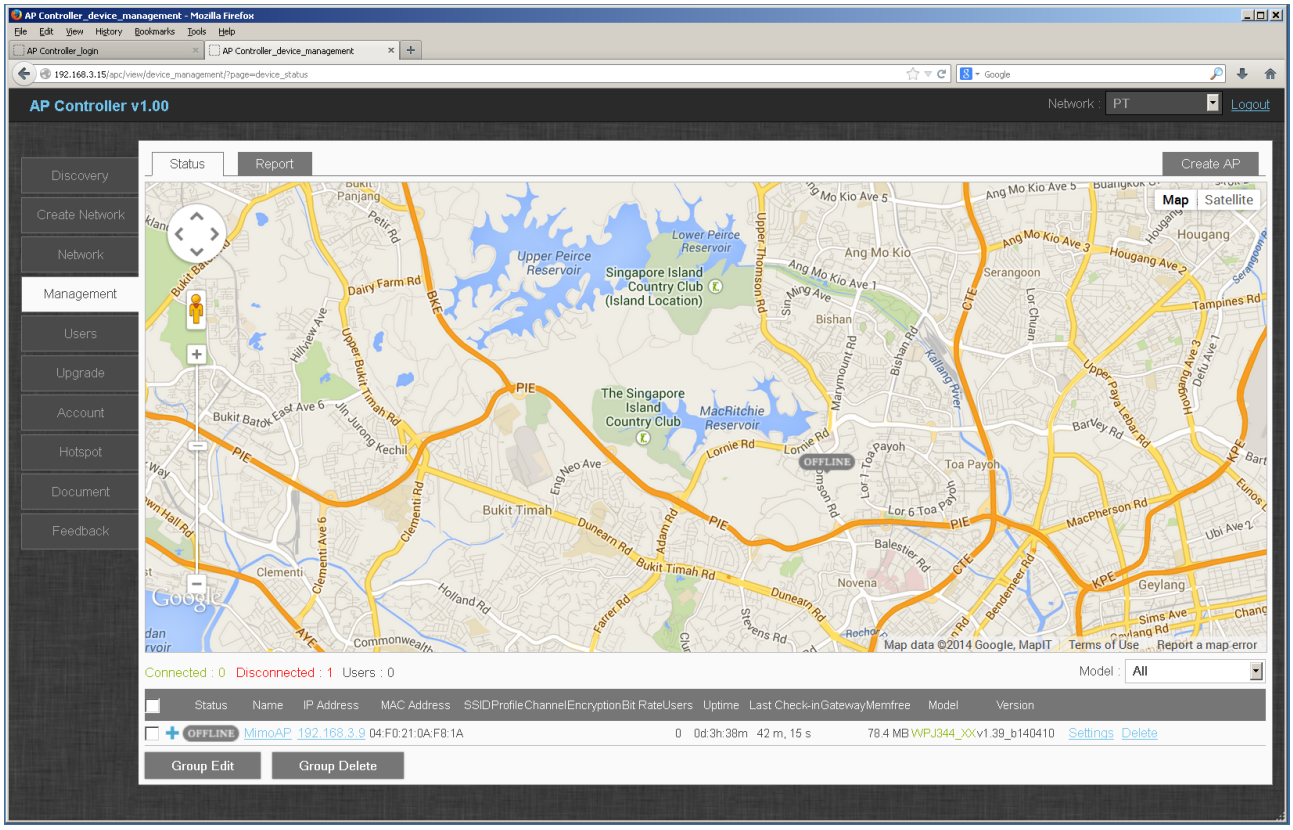


Figure 11: The [Management] page for the APc v1.00.

The [Management] page of the APc v1.04d is shown next.

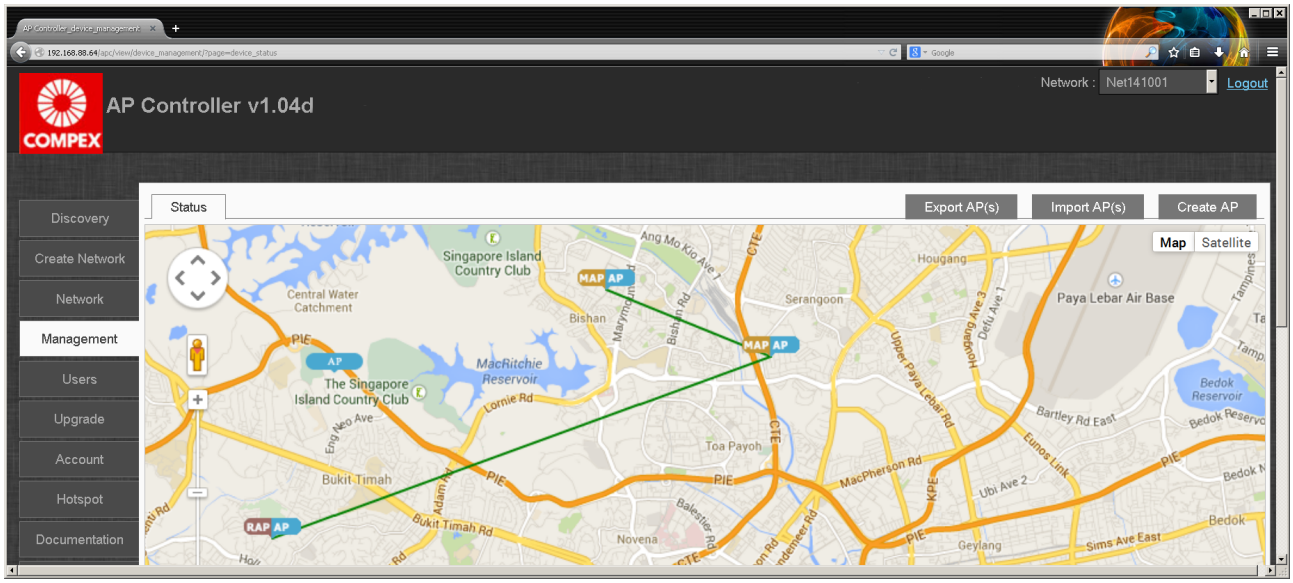


Figure 12: The [Management] page for the APc v1.04d, top half.

At the bottom of the page, you can see the Status table, and you can click on the plus (+) to show the VAPs.

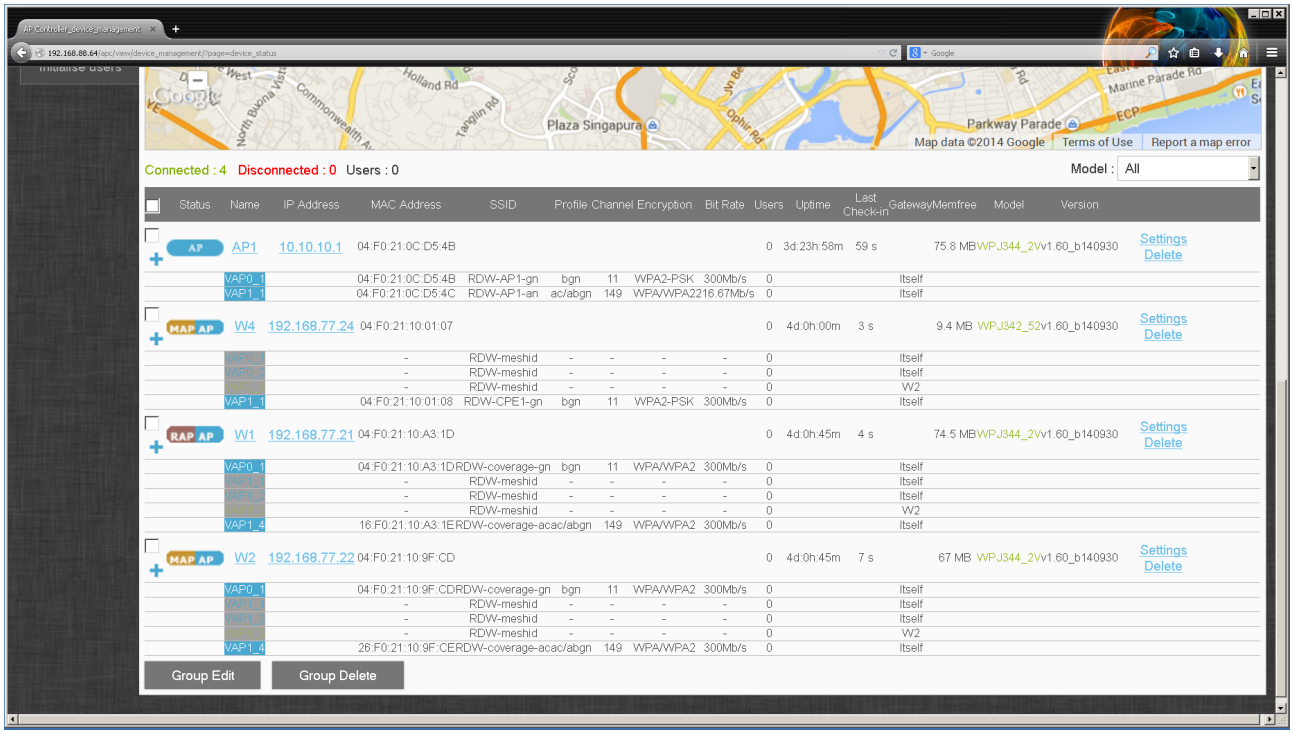

Connected : 4 Disconnected : 0 Users : 0
Model : All
Status Name IP Address MAC Address SSID Profile Channel Encryption Bit Rate Users Uptime Last Check-in Gateway Memfree Model Version
AP AP1 10.10.10.1 04:F0:21:0C:D5:4B 0 3d:23h:58m 59 s 75.8 MB WPJ344_2V v1.60_b140930 Settings Delete
VAP0_1 04:F0:21:0C:D5:4B RDW-AP1-gn bgn 11 WPA2-PSK 300Mb/s 0 Itself
VAP1_1 04:F0:21:0C:D5:4C RDW-AP1-an ac/abgn 149 WPA/WPA2 216.67Mb/s 0 Itself
MAP AP W4 192.168.77.24 04:F0:21:10:01:07 0 4d:0h:00m 3 s 9.4 MB WPJ342_52 v1.60_b140930 Settings Delete
VAP0_1 - RDW-meshid - - - - 0 Itself
VAP1_1 - RDW-meshid - - - - 0 Itself
VAP1_2 - RDW-meshid - - - - 0 W2
VAP1_1 04:F0:21:10:01:08 RDW-CPE1-gn bgn 11 WPA2-PSK 300Mb/s 0 Itself
RAP AP W1 192.168.77.21 04:F0:21:10:A3:1D 0 4d:0h:45m 4 s 74.5 MB WPJ344_2V v1.60_b140930 Settings Delete
VAP0_1 04:F0:21:10:A3:1D RDW-coverage-gn bgn 11 WPA/WPA2 300Mb/s 0 Itself
VAP1_1 - RDW-meshid - - - - 0 Itself
VAP1_2 - RDW-meshid - - - - 0 Itself
VAP1_3 - RDW-meshid - - - - 0 W2
VAP1_4 16:F0:21:10:A3:1E RDW-coverage-acac/abgn 149 WPA/WPA2 300Mb/s 0 Itself
MAP AP W2 192.168.77.22 04:F0:21:10:9F:CD 0 4d:0h:45m 7 s 67 MB WPJ344_2V v1.60_b140930 Settings Delete
VAP0_1 04:F0:21:10:9F:CD RDW-coverage-gn bgn 11 WPA/WPA2 300Mb/s 0 Itself
VAP1_1 - RDW-meshid - - - - 0 Itself
VAP1_2 - RDW-meshid - - - - 0 Itself
VAP1_3 - RDW-meshid - - - - 0 W2
VAP1_4 26:F0:21:10:9F:CE RDW-coverage-acac/abgn 149 WPA/WPA2 300Mb/s 0 Itself
Group Edit
Group Delete

Figure 13: The [Management] page for the APc v1.04d, bottom half.

The VAPs that are available for use are shown with a blue colour, otherwise they are shown with a grey colour.

More details on the Status table would be given later.

To add APs into the APc network, please go to the [Discovery] page and perform a scan.

6.1 The Export / Import / Create AP Tabs

At the top right corner of the [Management] page, we can see the following tabs:

- Export AP(s)
- Import AP(s)
- Create AP

6.1.1 The Export AP(s) Tab

This tab allows you to save the important details of the APs into a .csv file.

The following table provides an example of the .csv file.

AP1	04:F0:21:0C:D5:4B	WPJ344	2	V	1.344671772	103.7988281	admin	password	password

W4	04:F0:21:10:01:07	WPJ342	5	2	1.356684729	103.8379669	admin	password	password
W1	04:F0:21:10:A3:1D	WPJ344	2	V	1.320988911	103.7899017	admin	password	password
W2	04:F0:21:10:9F:CD	WPJ344	2	V	1.347074368	103.8616562	admin	password	password

For the .csv file, the column header details are as follows:

- AP name
- MAC address
- PCB model
  - Model of the printed circuit board (e.g. WPJ344)
- Radio 1
  - First radio (wifi0) radio type: V, 5, 2, or X.
    - 5GHz 11ac (V)
    - 5GHz 11n (5)
    - 2.4GHz 11n (2)
    - 5GHz/2.4GHz 11n (X)
  - This is the onboard radio if the onboard radio is enabled.
  - If the onboard radio is disabled, the first radio (wifi0) is the card radio.
- Radio 2
  - Second radio (wifi1) radio type: V, 5, 2, X, or 0.
  - 0 means there is no second radio.
- Latitude
- Longitude
- SNMPv3 username
- SNMPv3 authentication password
- SNMPv3 privacy password

This same file can be used for the “Import AP(s)” tab.

6.1.2 The Import AP(s) Tab

Suppose that the APs have been deleted from the APc network, or the APc had been reset.

The APs can be restored into the APc network by importing the same .csv file exported earlier. They would be placed in the original positions on the Google map.

The MAC address must be of a valid kind starting with 00:80:48 or 04:F0:21 or 00:24:A6 or 50:11:EB as these belong to Compex.

After clicking the button “Start Import”, click “OK” to go back to the [Management] page.

The newly imported APs should show up in the [Management] page in less than 2 minutes. You may also press the “F5” key to refresh the browser.

Please check that the model of each board (under the “Model” column) shows up as green words. If there are any errors, the model would show up as red words with “!?”.

6.1.3 The Create AP Tab

Sometimes you may want to create an entry for an AP in the [Management] page, even before the AP connects to the network. This can be done with the “Create AP” tab at the top right corner of the [Management] page.

The “Create AP” page is then displayed.

The following fields must be entered correctly in order for the AP to check-in later.

Hardware Settings

- Name (e.g. MimoAP)
- MAC Address
  - This must match the AP's MAC address.
  - The MAC address of wifi0 should be used, because it does not change. The other MAC addresses may change.
  - This MAC address is also written on the AP's product box.
  - The MAC address can also be seen by running the command, `ifconfig wifi0`, in the Linux shell of the AP. For example, in Figure 14, the MAC address is 04:F0:21:07:D9:D8. We take the first six pairs of characters and replace each dash “`-`” with a colon “`:`”
- Coverage (e.g. No)
- PCB
  - This must match the model of the AP's printed circuit board (PCB).
- Choices for PCB:
  - WPJ558
  - WPJ344
  - WPJ342
  - WPJ531
  - WPJ543

- WP546
- WPE72
- WPJ72

- Radio 1
  - This must match the type of the AP's first radio (wifi0).
- Radio 2
  - This must match the type of the AP's second radio (wifi1).
  - Choose 'None' if there is no second radio.
- Choices for the Radio 1 or Radio 2:
  - 5GHz 11ac (V)
  - 5GHz 11n (5)
  - 2.4GHz 11n (2)
  - 5GHz/2.4GHz 11n (X)

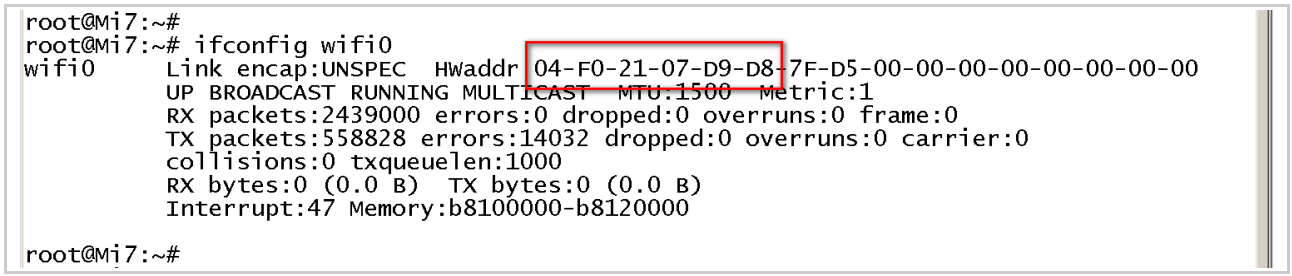

root@Mi7:~#
root@Mi7:~# ifconfig wifi0
wifi0 Link encap:UNSPEC HWaddr 04-F0-21-07-D9-D8-7F-D5-00-00-00-00-00-00-00-00
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2439000 errors:0 dropped:0 overruns:0 frame:0
TX packets:558828 errors:14032 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
Interrupt:47 Memory:b8100000-b8120000
root@Mi7:~#

Figure 14: The MAC address of an AP.

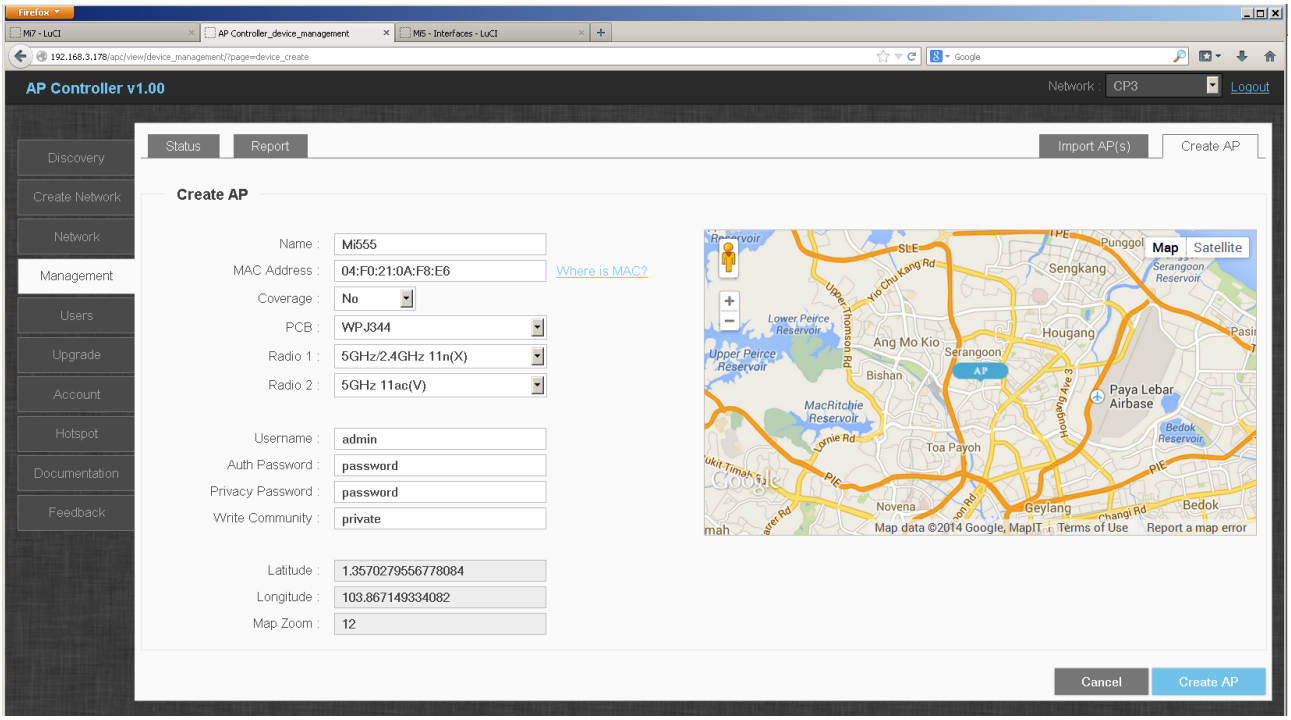
AP SNMPv3 Settings

- Username
- Auth Password
- Privacy Password

The default values for the AP SNMP settings are given in Section 9.3.2 AP SNMP Settings.

Position Settings

- Latitude (Drag the icon on the map.)
- Longitude (Drag the icon on the map.)
- Map Zoom (e.g. 12)



Click on the “Create AP” button at the bottom right corner. This would bring you to the main [Management] page.

The APc would then notify you when the AP connects to the network. This may take up to 2 minutes.

If there were any errors in the “PCB” , “Radio 1”, or “Radio 2” fields, the model of the board would show up as red text with “!?” e.g. “WPJ344_X !?”. Hovering the mouse cursor over this text would tell us, “Device cannot check-in because of that model settings conflict with device model.” You would have to delete this AP. You may “Create AP” again. Alternatively, go to the [Discovery] page to scan for new APs, because this AP is already connected.

6.2 Monitoring

The Google Map or Custom Map allows the customer to place their APs.

The APc displays each individual AP's statistics such as the IP address, MAC address, model of the board, and version of the firmware.

The APc also monitors each individual AP's status such as the virtual AP (VAP) status, uptime, time since the last check-in, and free memory.

The [Management] page updates every 15 seconds. (At present, the map and the table may refresh at different times because of different processes.)

6.2.1 Status Table

If an AP is online, its Status / Mode icon would be shown in the Status column, e.g. “AP”, “CPE”, or “AP | CPE”.

Each AP is expected to check-in every minute. If an AP does not check in after 1 minute, it is considered as offline, and its Status / Mode icon would show “OFFLINE”.

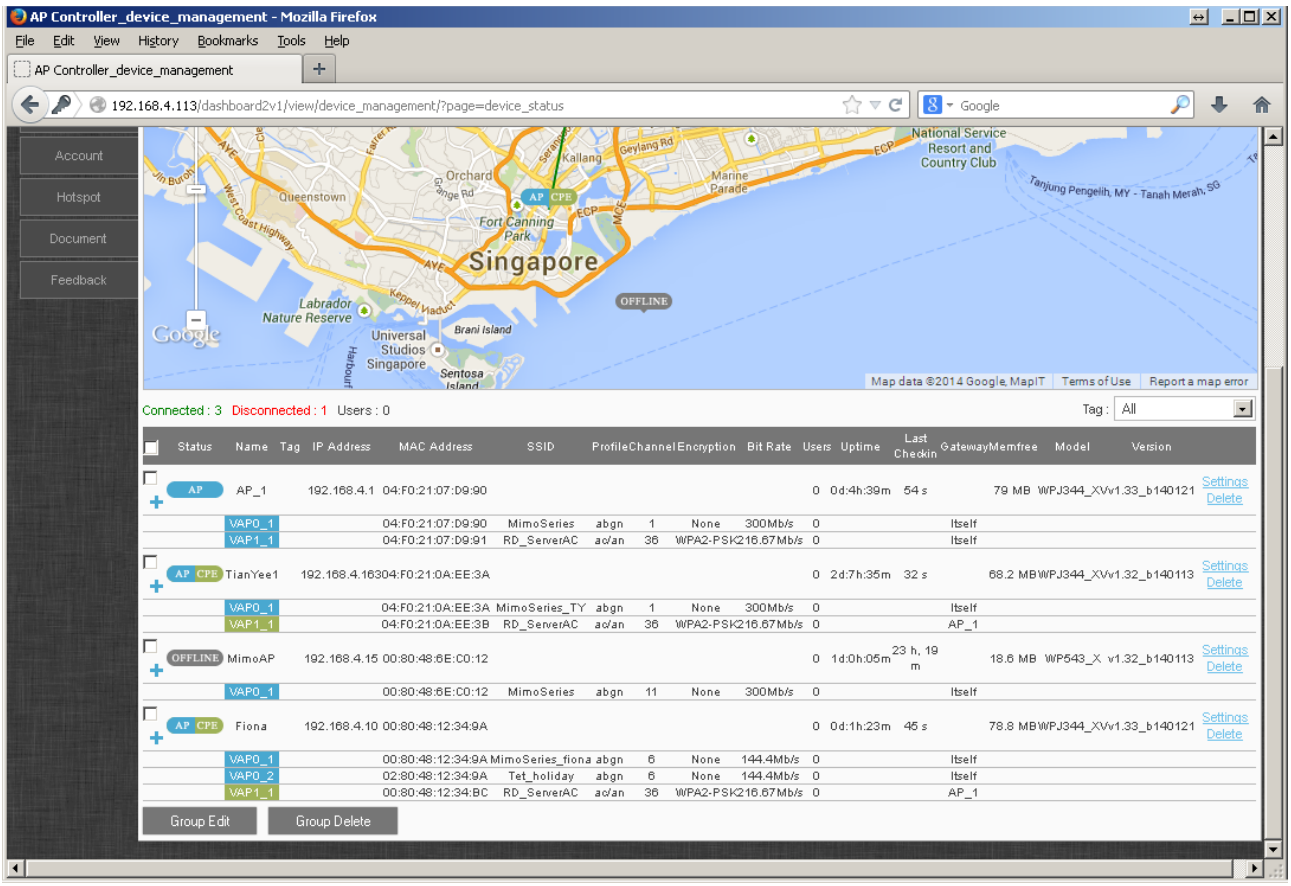

AP Controller_device_management - Mozilla Firefox
File Edit View History Bookmarks Tools Help
AP Controller_device_management
192.168.4.113/dashboard2v1/view/device_management/?page=device_status
Account
Hotspot
Document
Feedback
Singapore
OFFLINE
Connected : 3 Disconnected : 1 Users : 0
Tag : All
Status Name Tag IP Address MAC Address SSID Profile Channel Encryption Bit Rate Users Uptime Last Checkin Gateway Memfree Model Version
AP AP_1 192.168.4.1 04:F0:21:07:D9:90 0 0d:4h:39m 54 s 79 MB WPJ344_XVv1.33_b140121 Settings Delete
VAP0_1 04:F0:21:07:D9:90 MimoSeries abgn 1 None 300Mb/s 0 Itself
VAP1_1 04:F0:21:07:D9:91 RD_ServerAC ac/an 36 WPA2-PSK 216.67Mb/s 0 Itself
AP CPE TianYee1 192.168.4.163 04:F0:21:0A:EE:3A 0 2d:7h:35m 32 s 68.2 MB WPJ344_XVv1.32_b140113 Settings Delete
VAP0_1 04:F0:21:0A:EE:3A MimoSeries_TY abgn 1 None 300Mb/s 0 Itself
VAP1_1 04:F0:21:0A:EE:3B RD_ServerAC ac/an 36 WPA2-PSK 216.67Mb/s 0 AP_1
OFFLINE MimoAP 192.168.4.15 00:80:48:6E:C0:12 0 1d:0h:05m 23 h, 19 m 18.6 MB WP543_X v1.32_b140113 Settings Delete
VAP0_1 00:80:48:6E:C0:12 MimoSeries abgn 11 None 300Mb/s 0 Itself
AP CPE Fiona 192.168.4.10 00:80:48:12:34:9A 0 0d:1h:23m 45 s 78.8 MB WPJ344_XVv1.33_b140121 Settings Delete
VAP0_1 00:80:48:12:34:9A MimoSeries_fiona abgn 6 None 144.4Mb/s 0 Itself
VAP0_2 02:80:48:12:34:9A Tet_holiday abgn 6 None 144.4Mb/s 0 Itself
VAP1_1 00:80:48:12:34:BC RD_ServerAC ac/an 36 WPA2-PSK 216.67Mb/s 0 AP_1
Group Edit
Group Delete

Figure 15: Click the plus “+” icon for a router to reveal the VAP statistics.

Click the plus “+” icon for an AP to display the VAP statistics. These include the MAC address, SSID, channel, encryption, and bit rate.

Note on IP Address

The APc is able to manage APs on internal LAN networks by routing Layer 3 packets over the Layer 2 Tunnelling Protocol (L2TP).

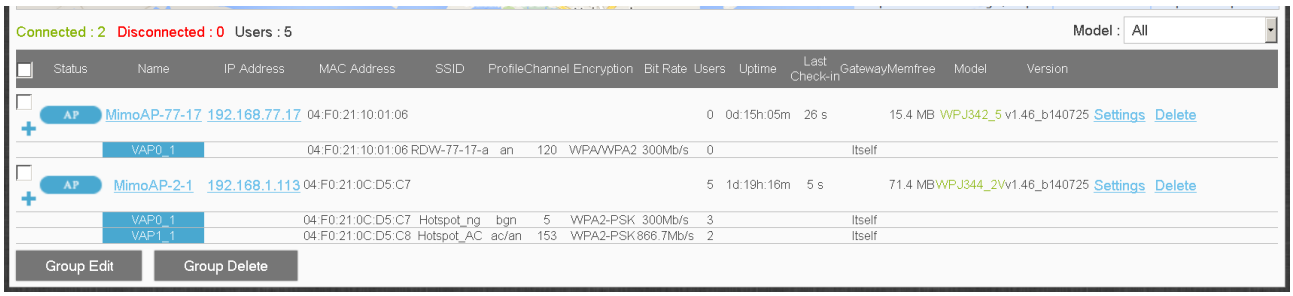

Connected : 2 Disconnected : 0 Users : 5
Model : All
Status Name IP Address MAC Address SSID Profile Channel Encryption Bit Rate Users Uptime Last Check-in Gateway Memfree Model Version
AP MimoAP-77-17 192.168.77.17 04:F0:21:10:01:06 0 0d:15h:05m 26 s 15.4 MB WPJ342_5 v1.46_b140725 Settings Delete
VAP0_1 04:F0:21:10:01:06 RDW-77-17-a an 120 WPA/WPA2 300Mb/s 0 Itself
AP MimoAP-2-1 192.168.1.113 04:F0:21:0C:D5:C7 5 1d:19h:16m 5 s 71.4 MB WPJ344_2V v1.46_b140725 Settings Delete
VAP0_1 04:F0:21:0C:D5:C7 Hotspot_ng bgn 5 WPA2-PSK 300Mb/s 3 Itself
VAP1_1 04:F0:21:0C:D5:C8 Hotspot_AC ac/an 153 WPA2-PSK 866.7Mb/s 2 Itself
Group Edit
Group Delete

Figure 16: If Hotspot is disabled, the LAN IP address is shown. If Hotspot is enabled, the WAN IP address is shown.

If the Hotspot service is disabled (default) on the AP, the LAN IP address of the AP is shown. If the Hotspot service is enabled on the AP, the WAN IP address of the AP is shown.

6.2.2 Pop-up box for an AP

The APc monitors end users (e.g. mobile phone, laptop) connected to the AP as well as the CompexWRT stations connected to the AP.

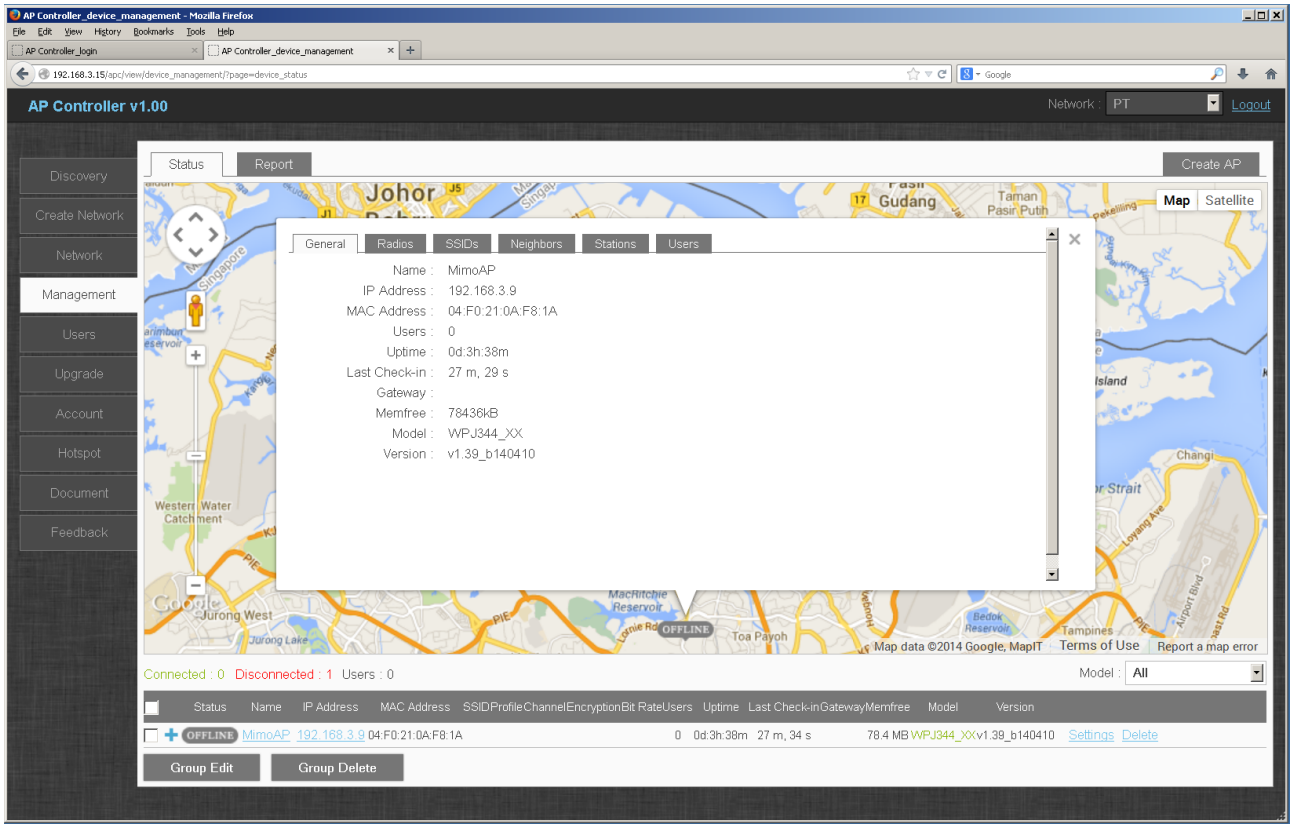


Figure 17: Click on the AP's name e.g. “MimoAP” to show a pop-up box with more details.

Clicking on the name of an AP e.g. “MimoAP” would bring up a pop-up box with the following tabs: General, Radios, SSIDs, Neighbors, Stations, and Users. These tabs are described as follows.

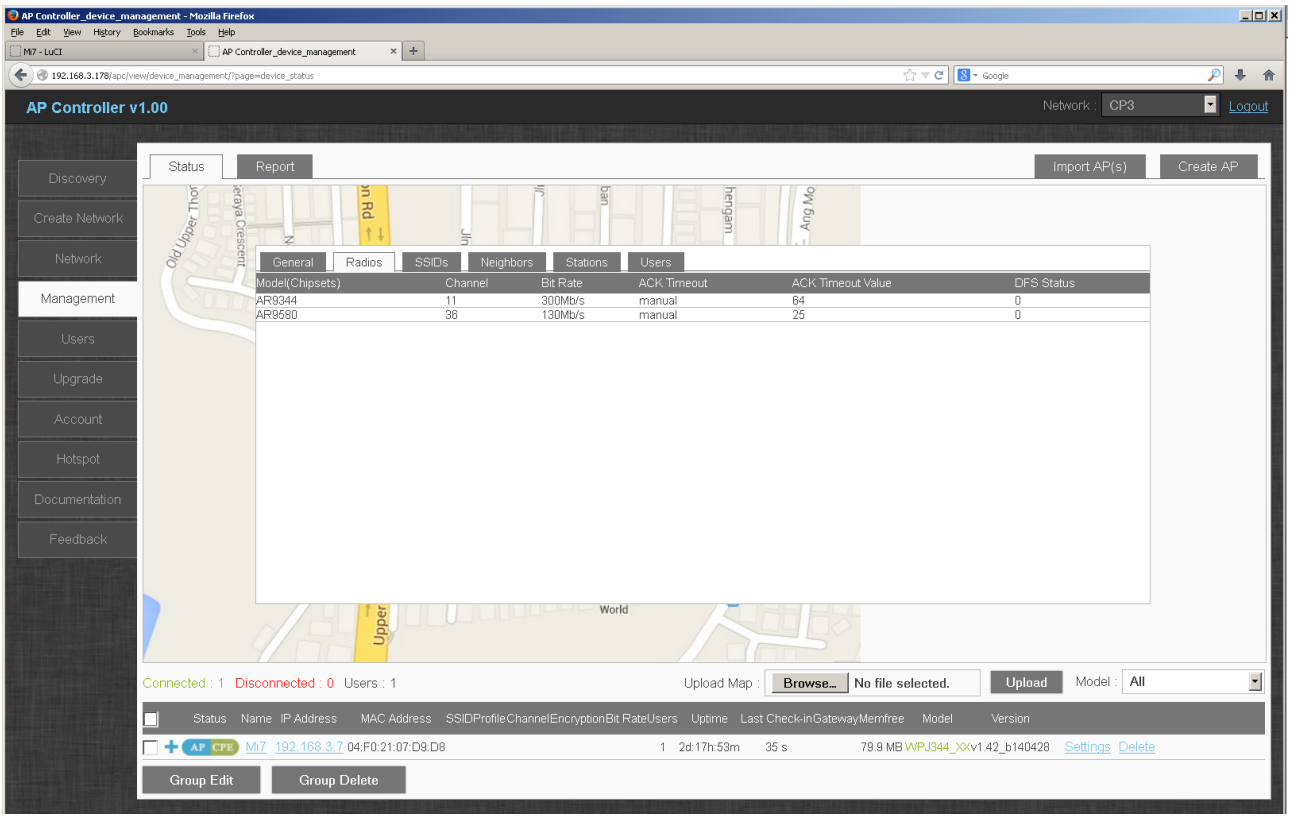
General

In the General tab of the pop-up box, the details could be for example:

Name :	MimoAP
IP Address :	192.168.3.8
MAC Address :	04:F0:21:15:21:58
Users :	3
Uptime :	0d:0h:10m
Last Check-in :	12 s
Gateway :	192.168.3.1
Memfree :	80712kB
Model :	WPJ344_X
Version :	v1.39_b140401

Radios

In the “Radios” tab, the radios are listed in a table and the following parameters are shown: Model(Chipsets), Channel, Bit Rate, ACK Timeout, and ACK Timeout Value.



SSIDs

In the SSIDs tab, the list of wireless networks (SSIDs) are displayed in a table with the following parameters: SSID, Profile, Channel, Encryption, and TX Rate/RX Rate.

Neighbors

In the “Neighbors” tab, a table shows the details: Status, Name, MAC Address, IP Address, and Signal. This would be relevant to the Compex MeshWRT.

Stations

In the Stations tab, the connected end users and CompexWRT stations are listed in a table. The parameters shown are: Host, IP Address, MAC Address, Network, Signal, Signal/Chains, TX Rate, RX Rate, and TX-CCQ. The list of stations is updated every 1 minute.

Users

In the Users tab, the list of end users (e.g. mobile phone, laptop) is displayed in table with the following parameters: Host, IP Address, MAC Address, Brand, Network, Signal, Signal/Chains, TX Rate, RX Rate, Upload(MB), Download(MB), Total(MB). The list of end users is updated every 15 seconds.

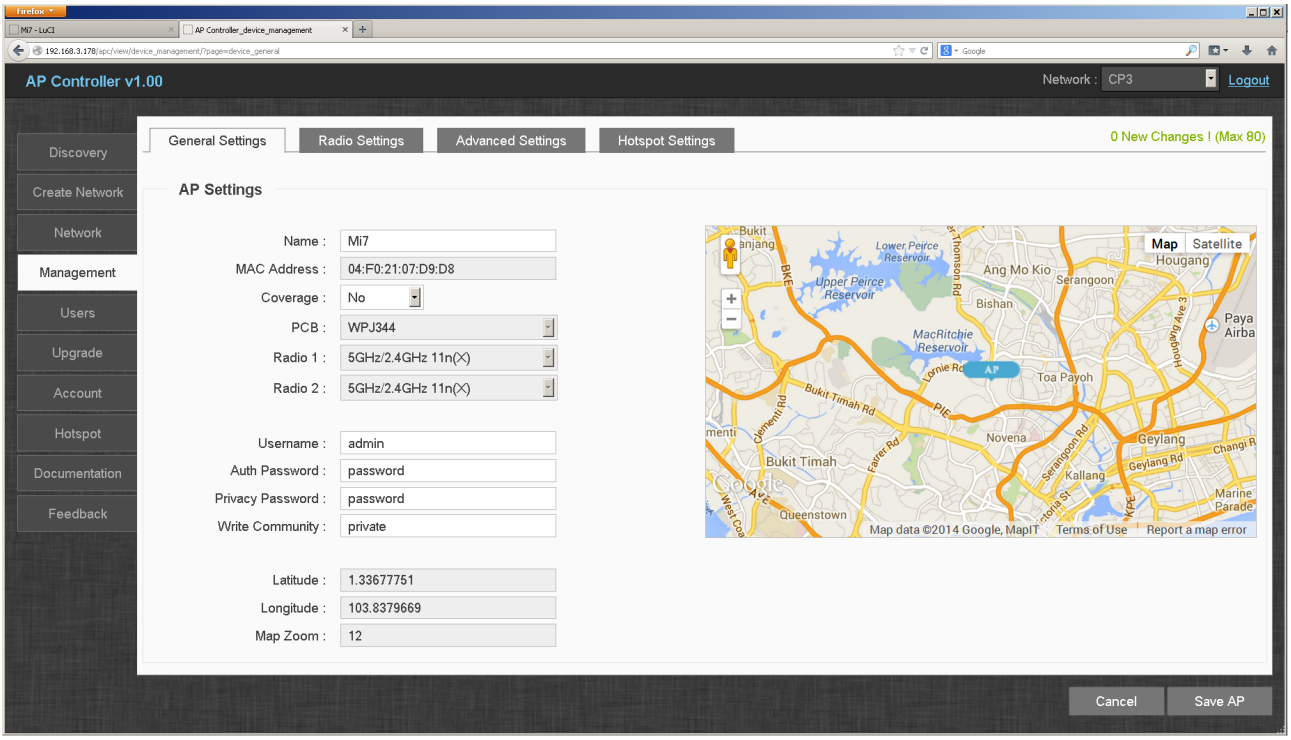
6.3 Changing the Settings of an AP

The APc can be used to configure the settings of an AP. In the Status table, click “Settings” on the row showing the details of the AP.

A new page is displayed, with the following tabs at the top:

- General Settings
- Radio Settings
- Advanced Settings
- Hotspot Settings

Note: If you made any changes, remember to click the button “Save AP” or “Save Settings” at the bottom right corner before switching tabs. This is to save the changes.



6.3.1 General Settings

The following lists the parameters displayed under the “General Settings” tab.

Hardware Settings

- Name
- MAC Address (Cannot be changed after adding AP.)
- Coverage
- PCB (Cannot be changed after adding AP.)
- Radio 1 (Cannot be changed manually after adding AP.)
- Radio 2 (Cannot be changed manually after adding AP.)

AP SNMP Settings

The default settings are given in Section 9.3.2 AP SNMP Settings.

To be implemented: These settings could be different for different APs. They would need to match with the *AP SNMP Settings* on each AP. Due to security reasons, these settings cannot be transferred from the APc to the AP. They would need to be configured on both the APc and the APs.

Position Settings

- Latitude (Drag the icon on the map.)
- Longitude (Drag the icon on the map.)
- Map Zoom (e.g. 12)

6.3.2 Radio Settings

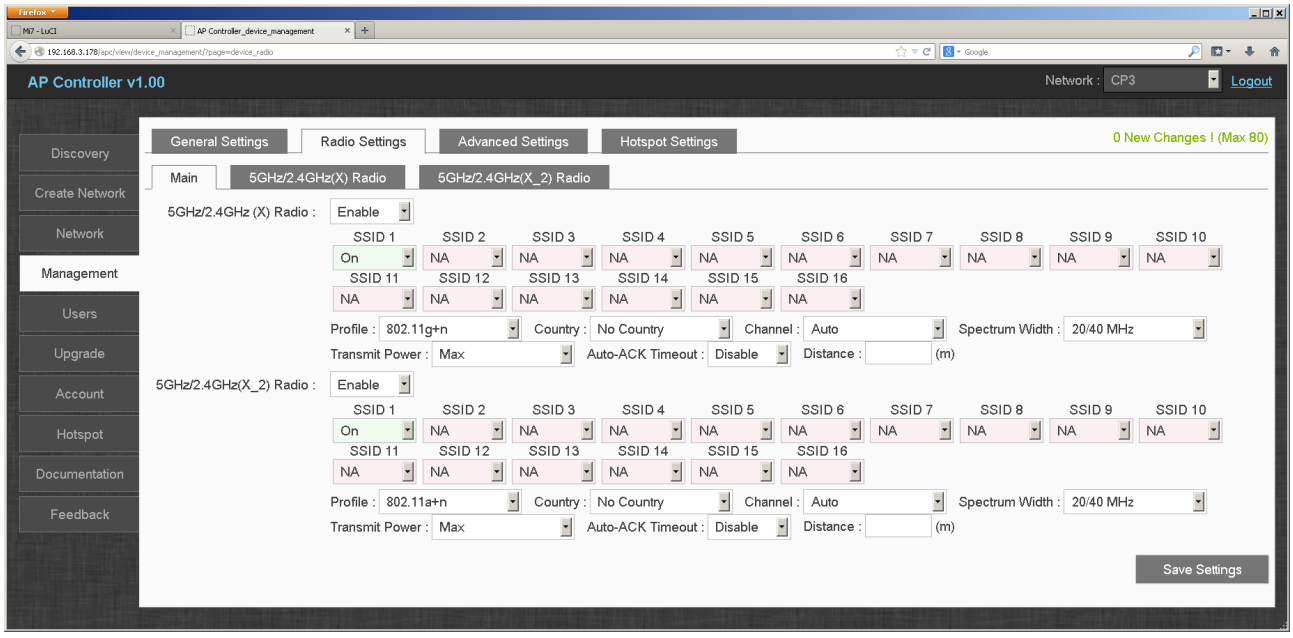
Under the “Radio Settings” top-level tab, there are a number of second-level tabs, for example:

- Main
- Tab for the First Radio e.g. '5GHz/2.4GHz(X) Radio'
- Tab for the Second Radio e.g. '5GHz/2.4GHz(X_2) Radio'

These second-level tabs are explained as follows.

Main

On this tab, all the radios of the AP are shown.


AP Controller v1.00
Network : CP3
Logout
Discovery
Create Network
Network
Management
Users
Upgrade
Account
Hotspot
Documentation
Feedback
General Settings
Radio Settings
Advanced Settings
Hotspot Settings
0 New Changes ! (Max 80)
Main
5GHz/2.4GHz(X) Radio
5GHz/2.4GHz(X_2) Radio
5GHz/2.4GHz (X) Radio :
Enable
SSID 1 SSID 2 SSID 3 SSID 4 SSID 5 SSID 6 SSID 7 SSID 8 SSID 9 SSID 10
On NA NA NA NA NA NA NA NA NA
SSID 11 SSID 12 SSID 13 SSID 14 SSID 15 SSID 16
NA NA NA NA NA NA
Profile : 802.11g+n
Country : No Country
Channel : Auto
Spectrum Width : 20/40 MHz
Transmit Power : Max
Auto-ACK Timeout : Disable
Distance : (m)
5GHz/2.4GHz(X_2) Radio :
Enable
SSID 1 SSID 2 SSID 3 SSID 4 SSID 5 SSID 6 SSID 7 SSID 8 SSID 9 SSID 10
On NA NA NA NA NA NA NA NA NA
SSID 11 SSID 12 SSID 13 SSID 14 SSID 15 SSID 16
NA NA NA NA NA NA
Profile : 802.11a+n
Country : No Country
Channel : Auto
Spectrum Width : 20/40 MHz
Transmit Power : Max
Auto-ACK Timeout : Disable
Distance : (m)
Save Settings

For each radio, you can enable or disable it.

Up to 16 SSIDs/VAPs can be created for each radio.

For each SSID, you can enable it, disable it, or delete it.

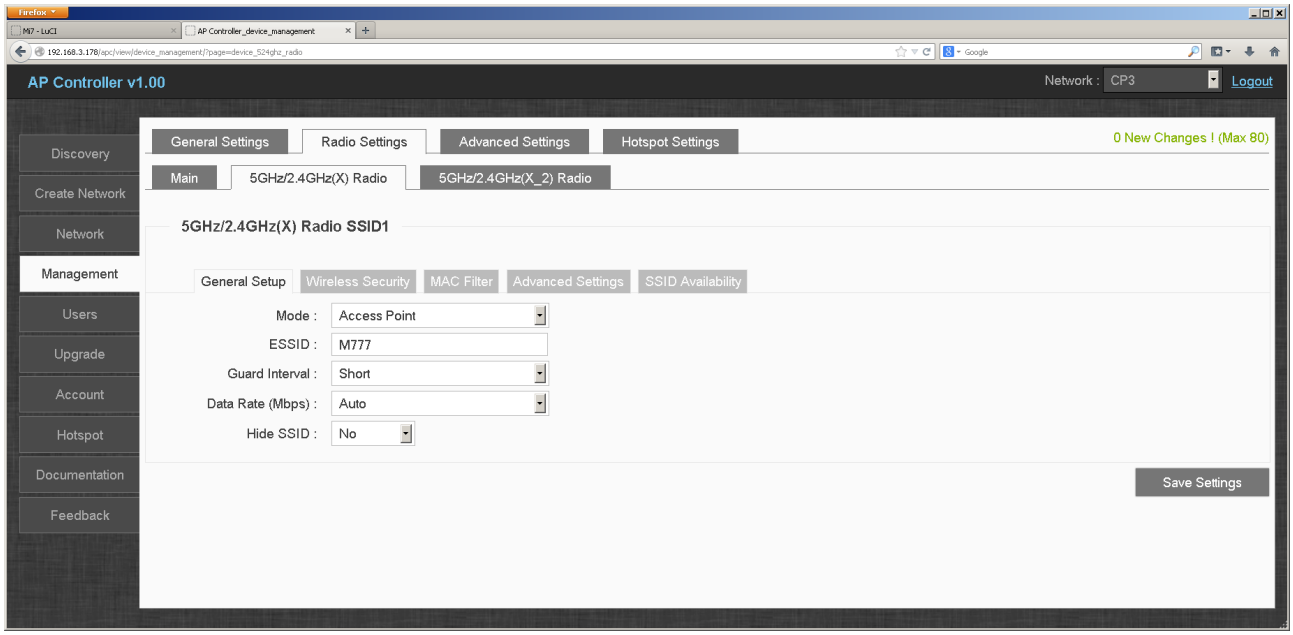
Other options include:

- Profile (wireless profile, for example 802.11g+n, 802.11a+n, or 802.11ac)
- Country (Note: This has no relation to the “Location” setting of the APc network)
- Channel
- Spectrum Width (for example 20 MHz, 20/40 MHz, or 20/40/80 MHz)
- Transmit Power (for example 'Max')
- Auto-ACK Timeout (Auto or Disable)
- Distance (m)

Tab for the First Radio e.g. '5GHz/2.4GHz(X) Radio'

For each SSID, the following sub-tabs are shown:

- General Setup
- Wireless Security
- MAC Filter (for AP mode only)
- Advanced Settings
- SSID Availability



The tabs and their options are listed as follows.

General Setup

- Mode (Access Point, Access Point WDS, Station, or Station WDS)

- ESSID (This is the name of the wireless network, or SSID.)
- Guard Interval (default: Short)
- Data Rate (Mbps) (default: Auto)
- Hide SSID (default: No)

Wireless Security

- Wireless Security: This may be 'No Encryption' or a particular wireless encryption such as
  - WPA-PSK
  - WPA2-PSK
  - WPA/WPA2-PSK
  - WPA/EAP
  - WPA2/EAP
- Cipher: The choices are
  - Auto
  - CCMP(AES)
  - TKIP and CCMP(AES)
- Key
  - 8 to 63 printable ASCII characters, no space " ", and no ampersand "&".

MAC Filter (for AP mode only)

- MAC ACL (Access control list, default: Disable)

Advanced Settings

- RTS Threshold (default: blank)
- Station Isolation (for AP mode only, default: disable)
- Maximum Stations (for AP mode only, default: blank)
- Minimum Stations RSSI (for AP mode only, default: blank)
- 802.11n/802.11ac Only (for AP mode only, default: disable)
- HT20/HT40 Coexistence (default: Disable)

- WMM (default: Enable)

SSID Availability (Future Feature)

- Scheduled Availability (default: Disable)
- Scheduled Templates

Day	Availability	From	To
Sunday			
Monday			
Tuesday			
Wednesday			
Thursday			
Friday			
Saturday			

Tab for the Second Radio e.g. '5GHz/2.4GHz(X_2) Radio'

The parameters in the tab for each radio are the same. The reader may refer to the previous section.

6.3.3 Advanced Settings

- SSH Passwords
  - You may enter a new password for the “root” user of the CompexWRT AP's Linux shell.
- Web (default: Enable)
- Failover AP Controller (This is normally used for monitoring only.)

6.3.4 Hotspot Settings (x)

(Currently, if you disable all the wireless on the hotspot router, it should not be checked in to the APc because the icons on the [Management] page map would have errors.)

The Hotspot Settings tab contains three sub-tabs:

- General Settings

- Network Configuration
- Radius Configuration

The options within are described as follows.

General Settings

- Enable Hotspot (default: Disable)
    - You may wish to enable Hotspot after all the settings are done.
- Hotspot Mode (Select your desired mode of Hotspot.)
    - User Name + Password (Radius Required)
    - Agreement (Radius Required)
    - Password (Radius Required)
    - Agreement (Radius not Required)
    - Password (Radius not Required)
- Login Page Title (Title shown on the Login Page)
- Idle Time Out (Default idle timeout or max idle time unless otherwise set by RADIUS. Set as 0 to mean unlimited time.)

Network Configuration

- Auto Config (default: Yes)

Radius Configuration

- Radius Server 1 : The IP address of radius server. The IP address of the APc can be used e.g. 192.168.3.178.
- Radius Server 2 : The IP address of radius server e.g. 192.168.3.178.
- Radius Secret : Radius shared secret for both servers. This secret should be changed in order not to compromise security. (default: test)
- UAM Server : URL of web server to use for authenticating clients:
    - e.g. http://192.168.3.178/apc/hotspot/login.html
- UAM Secret : Shared secret between uamserver and chilli. This secret should be set in order not to compromise security. (default: leave as blank)

- Walled Garden (Domain) : Comma separated list of resources the client can access without first authenticating. Each entry in the list is a domain name. Do not put www in the domain name. For example: google.com is good domain name, www.google.com is not acceptable. (default: coova.org)

- Walled Garden (IP Address) : Comma separated list of resources the client can access without first authenticating. Each entry in the list is an IP Address. The AP's web page is always accessible. The APc's web page is also always accessible.

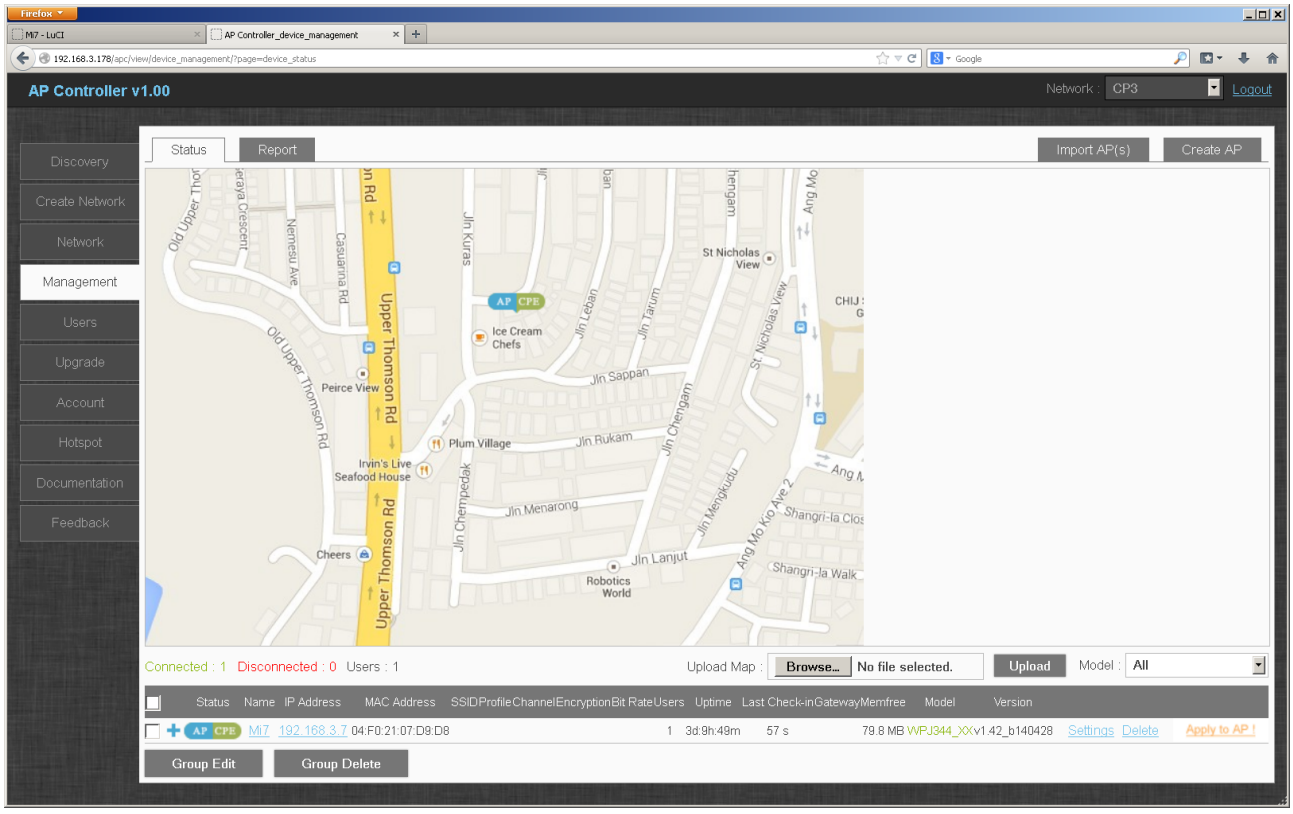
6.4 Saving the Settings of an AP

After you have made the changes, they would need to be saved and then applied.

Save the settings by clicking on the button “Save Settings” (or “Save AP”).

6.5 Applying the Settings to an AP

To apply the settings, click on the [Management] link on the left menu bar to go to the main [Management] page again. On the row showing the edited AP, there would appear a flashing button “Apply to AP”. Click this button to send the configuration changes you just made to the AP.



In less than 2 minutes, the AP should be updated and the status icon of the AP would be updated on the map as well as the table on the [Management] page.

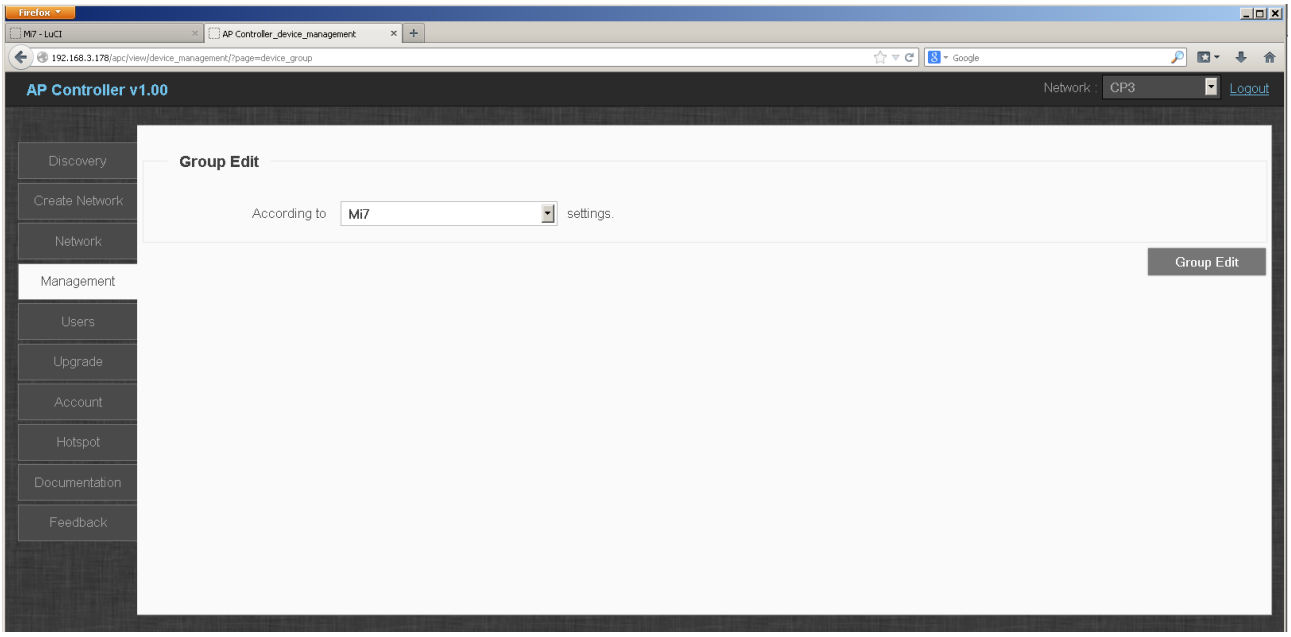
While applying the changes, the status icon for the AP may show “Applying”. If the AP still has not checked in after 4 minutes, it is considered as offline and the status icon for this AP would show “OFFLINE”.

6.6 Changing the Settings of Multiple APs Simultaneously

The “Group Edit” button allows you to apply settings for multiple selected APs at the same time.

According to [a particular AP's] settings.

- Select the AP for which you would take the settings as reference.



Refer to Section 6.3 *Changing the Settings of an AP*. The parameters described are also the same here.

Save the settings by clicking on the button “Save Settings” (or “Save AP”).

To apply the settings to each AP, refer to Section 6.5 *Applying the Settings to an AP*.

6.7 Mesh

A mesh network can be set up using CompexWRT APs. Using the BATMAN technology, the APs are able to provide wireless coverage. Redundancy is achieved because if one AP dies, the other APs would automatically link up and calculate the most efficient path.

A CompexWRT AP can be configured as one of the following three mesh modes:

- Root AP (RAP)
- Mesh AP (MAP)

- Root AP + Router Client (RRC)

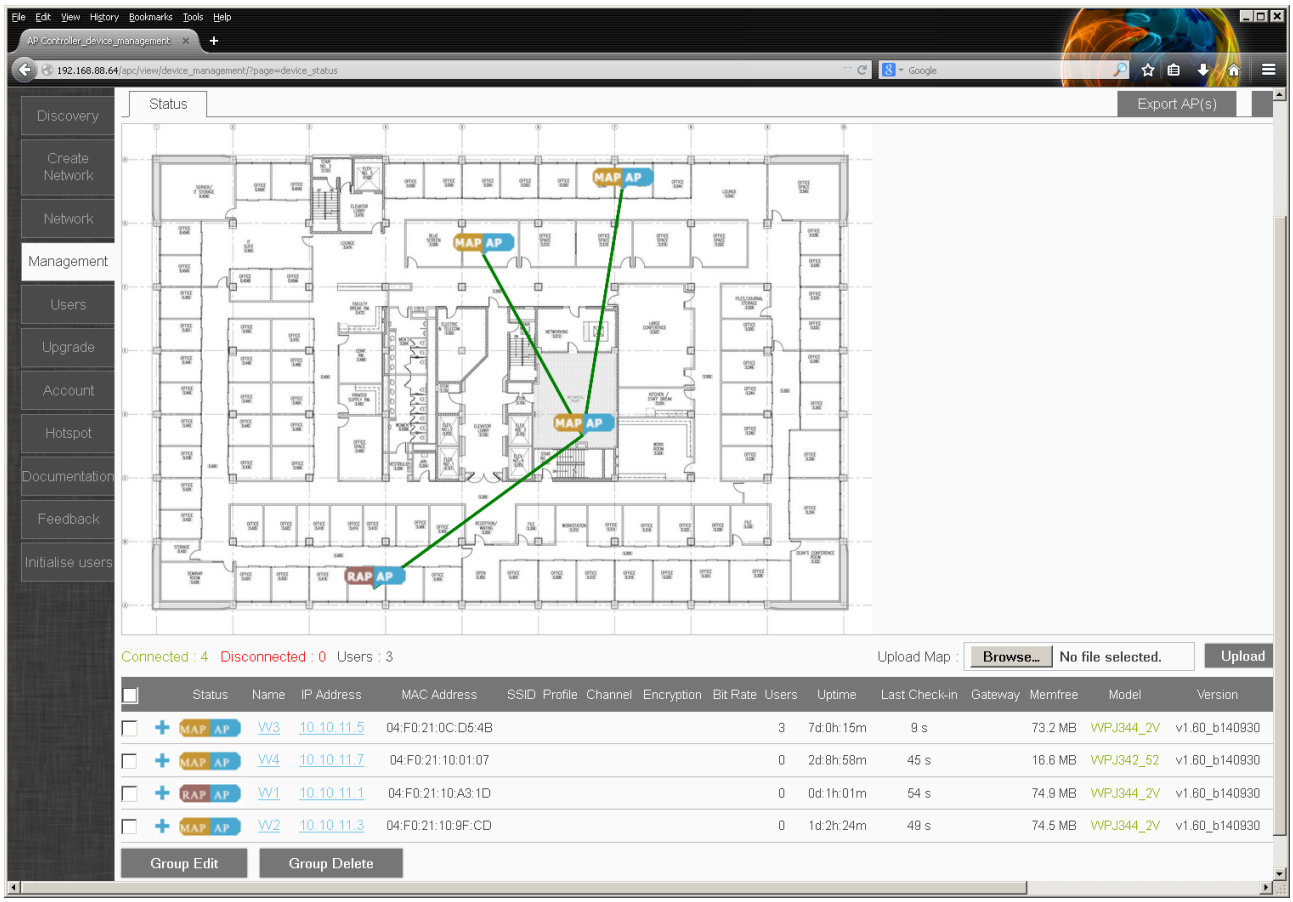


Figure 18: RAP W1 connected to MAP W2 in turn connected to W3 and W4.

An RAP is connected to the Internet or main network by a wired LAN connection and broadcasts a wireless mesh signal.

MAPs connect wirelessly in a mesh configuration and at least one MAP connects to an RAP.

This RAP functions like a gateway for the MAPs to connect to the Internet network.

A mesh network can have multiple RAPs.

Suppose that you already have an existing wireless router without the mesh capability, and already broadcasting on the same channel that you would use for the mesh. An RAP just beside this router would introduce an unnecessary wireless network. In this case, you can use an RRC placed some distance away.

An RRC functions as a station associated with the wireless network of the existing router. It then broadcasts the wireless mesh signal just like an RAP.

A mesh network can be set up using the AP Controller (APc). The steps are explained in the following section.

6.8 Steps to Set Up a Mesh Network

In a mesh network, all the APs have to use the same wireless profile (e.g. 802.11a+n), channel (e.g. 149), spectrum width (e.g. 20/40 MHz), and encryption (e.g. WPA/WPA2-PSK).

Note that the current version (v1.04d) of the APc cannot control the LAN and WAN settings of the APs. Therefore you can only create the mesh network using currently connected APs and stations. If you have new APs in factory default configuration, please refer to the CompexWRT user manual to configure the APs individually.

6.8.1 RAP Configuration

From the [Management] page, click on “Settings” for the AP that you would use as the root AP (RAP). It should be connected to the Internet network by a LAN cable.

In the Radio Settings > Main tab, enable the mesh for a radio e.g. the AC (V) Radio, by selecting “Enable” for the “Mesh” option.

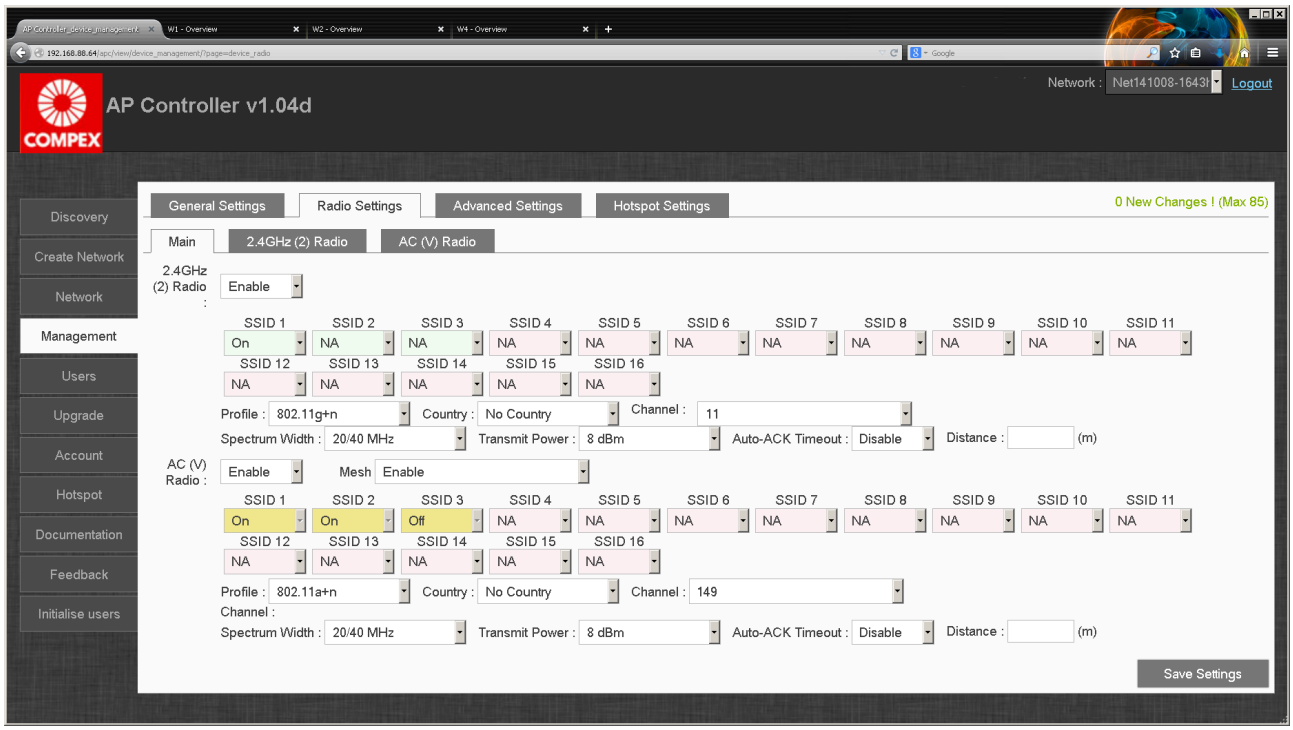


Figure 19: Enable Mesh in the Radio Settings > Main page.

Please select the wireless “Profile”, “Channel”, and “Spectrum Width” that should be common for all the mesh APs. Following that, please click the “Save Settings” button.

Next, click on the tab for the radio.

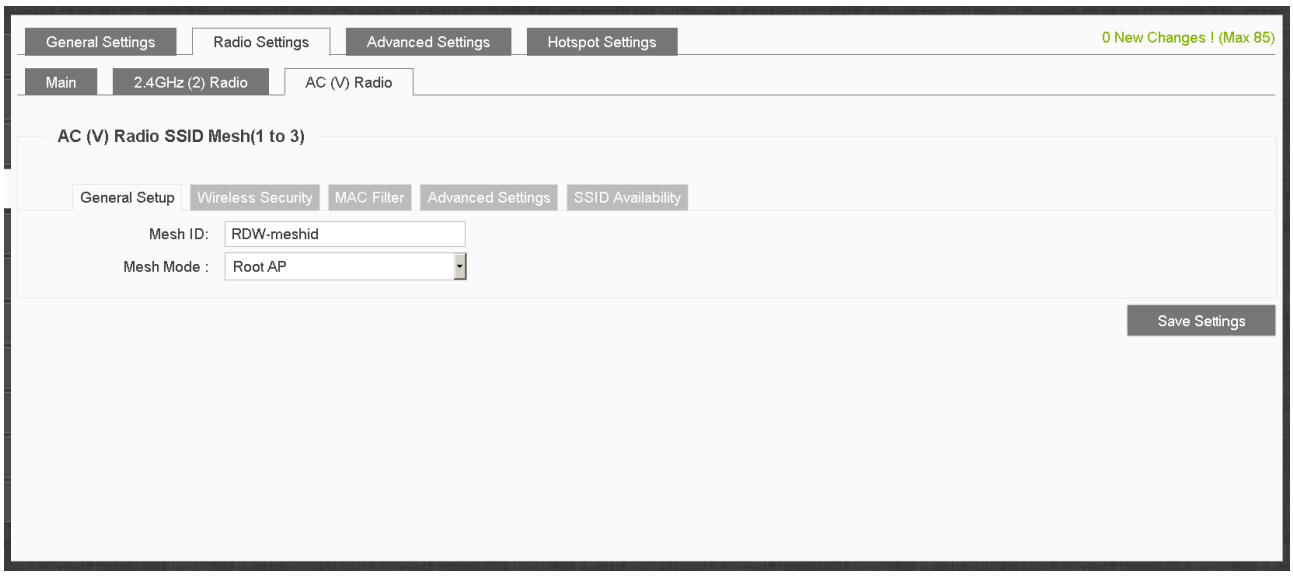


Figure 20: Mesh ID and Mesh Mode in the General Setup tab of the radio, RAP.

Mesh ID: Key in the Mesh ID that would identify this mesh. All the mesh APs would be linked by this common Mesh ID.

Mesh Mode: The available options are

- Mesh AP (MAP)
- Root AP (RAP)
- Root AP + Router Client (RRC)

Since this AP is to be a root AP, please select “Root AP”. You can have multiple root APs.

Then, please click the “Save Settings” button.

Next, click on the “Wireless Security” tab to set the wireless encryption settings (e.g. WPA/WPA2-PSK). These settings should be the same for all the APs in the mesh.

Please click on the “Save Settings” button whenever you make changes to any page.

After that, you may set up additional wireless networks on this AP to provide coverage.

You could create an additional wireless network on the same radio as the mesh network by adding a virtual AP (VAP).

You could also have a wireless network on the other radio to provide coverage for a different wireless profile (e.g. 802.11g+n).

Once the settings are completed for the RAP, click on the [Management] tab to go back to the main page.

6.8.2 RRC Configuration

The Root AP + Router Client (RRC) is not required if you are using an RAP.

The AP that is to be the RRC should not have any WAN interfaces. That is, it is operating in bridge mode. It should have a radio in station mode associated with your existing Internet network router. Your existing router should have the same wireless “Profile”, “Channel”, and “Spectrum Width” that would be common for all the mesh APs.

From the [Management] page, click on “Settings” for the AP that you would use as the RRC.

In the Radio Settings > Main tab, enable the mesh for a radio e.g. the AC (V) Radio, by selecting “Enable” for the “Mesh” option.

On the same page, please set the wireless “Profile”, “Channel”, and “Spectrum Width” options for this radio.

Following that, please click the “Save Settings” button.

Next, click on the tab for the radio.

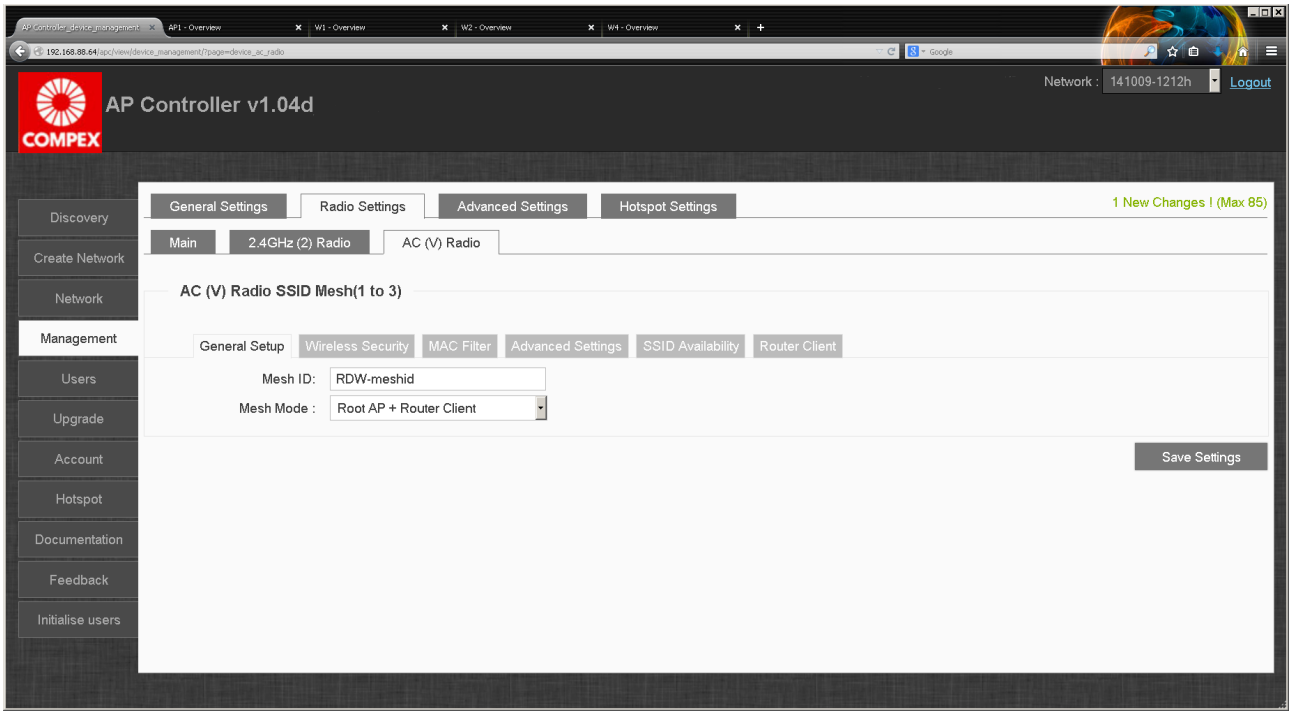


Figure 21: Mesh ID and Mesh Mode in the General Setup tab of the radio, RRC.

Mesh ID: Key in the Mesh ID that would identify this mesh. All the mesh APs would be linked by this common Mesh ID.

Mesh Mode: Please select “Root AP + Router Client”.

Then, please click the “Save Settings” button.

You would notice that a new tab “Router Client” shows up on the right side of the row of tabs.

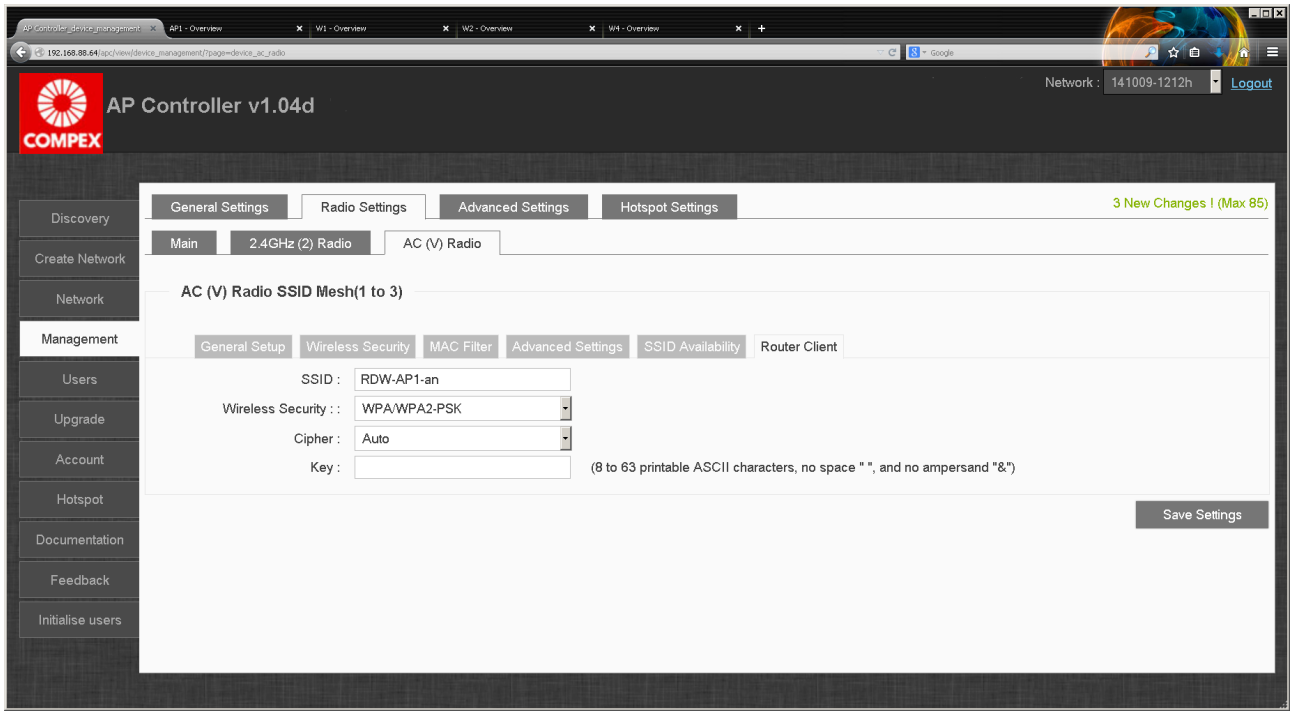


Figure 22: The “Router Client” tab of the RRC.

Please key in the SSID of your existing router, as well as its wireless security settings. Once this is done, please click “Save Settings”.

Next, click on the “Wireless Security” tab to set the wireless encryption settings (e.g. WPA/WPA2-PSK) of the mesh. These settings should be the same for all the APs in the mesh.

Please click on the “Save Settings” button whenever you make changes to any page.

After that, you may set up additional wireless networks on this AP to provide coverage. The steps are the same as for the RAP.

Once the settings are completed for the RRC, click on the [Management] tab to go back to the main page.

6.8.3 MAP Configuration

From the [Management] page, click on “Settings” for the AP that you would use as a mesh AP (MAP). This AP should not have any WAN interfaces. That is, it is operating in bridge mode.

In the Radio Settings > Main tab, enable the mesh for a radio e.g. the AC (V) Radio, by selecting “Enable” for the “Mesh” option.

On the same page, please set the wireless “Profile”, “Channel”, and “Spectrum Width” options for this radio.

Following that, please click the “Save Settings” button.

Next, click on the tab for the radio.

Mesh ID: Key in the Mesh ID that would identify this mesh. All the mesh APs would be linked by this common Mesh ID.

Mesh Mode: Please select “Mesh AP”.

Then, please click the “Save Settings” button.

Next, click on the “Wireless Security” tab to set the wireless encryption settings (e.g. WPA/WPA2-PSK) of the mesh. These settings should be the same for all the APs in the mesh.

Please click on the “Save Settings” button whenever you make changes to any page.

After that, you may set up additional wireless networks on this AP to provide coverage. The steps are the same as for the RAP.

Once the settings are completed for the MAP, click on the [Management] tab to go back to the main page.

Other MAPs can be configured in a similar fashion.

6.8.4 Apply the Settings to the APs

The next step is to send the configurations to the APs.

In the [Management] page, make sure the APs are online.

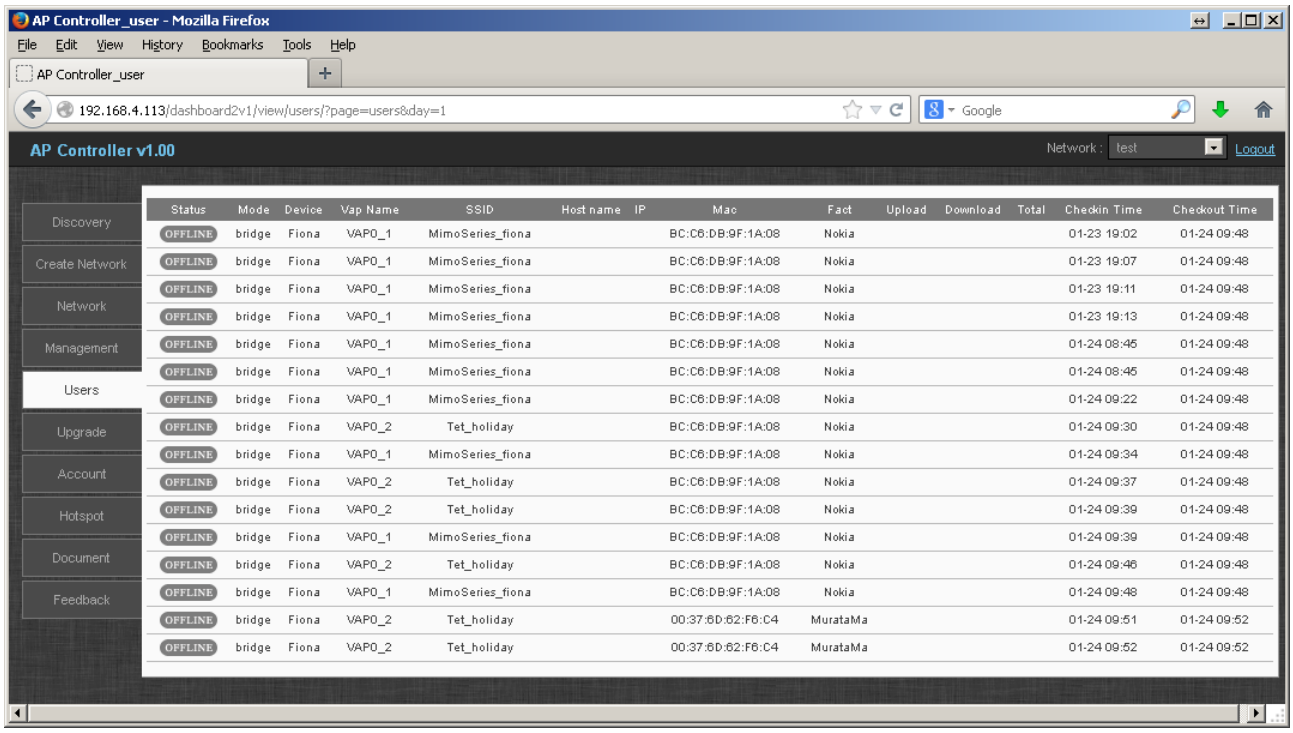
Click “Apply to AP” for the AP furthest away from the APc, then for the APs closer towards the APc in the network.

This will ensure that the configurations would be sent to all the APs as fast as possible.

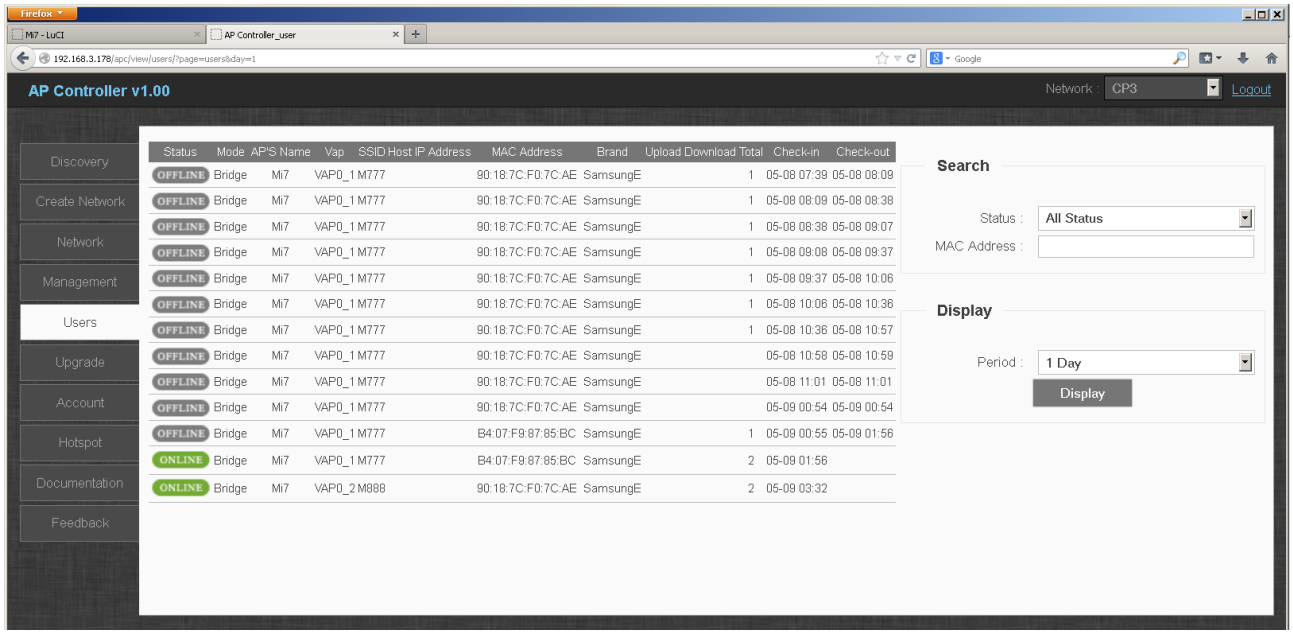
After that, wait for the APs to check-in to the APc again.

Section 7: The [Users] Page

The APc keeps a record of end users (devices e.g. mobile phone, laptop) connected to all the APs. The parameters shown include the MAC address, brand of the device, AP and SSID that it is connected to. The upload and download data usage, check-in and check-out times are shown. The end users are updated every 15 seconds. You can view the log of all the users up to 5 days.


AP Controller_user - Mozilla Firefox
File Edit View History Bookmarks Tools Help
AP Controller_user
192.168.4.113/dashboard2v1/view/users/?page=users&day=1
AP Controller v1.00
Network : test
Logout
Discovery
Create Network
Network
Management
Users
Upgrade
Account
Hotspot
Document
Feedback
Status Mode Device Vap Name SSID Host name IP Mac Fact Upload Download Total Checkin Time Checkout Time
OFFLINE bridge Fiona VAP0_1 MimoSeries_fiona BC:C6:DB:9F:1A:08 Nokia 01-23 19:02 01-24 09:48
OFFLINE bridge Fiona VAP0_1 MimoSeries_fiona BC:C6:DB:9F:1A:08 Nokia 01-23 19:07 01-24 09:48
OFFLINE bridge Fiona VAP0_1 MimoSeries_fiona BC:C6:DB:9F:1A:08 Nokia 01-23 19:11 01-24 09:48
OFFLINE bridge Fiona VAP0_1 MimoSeries_fiona BC:C6:DB:9F:1A:08 Nokia 01-23 19:13 01-24 09:48
OFFLINE bridge Fiona VAP0_1 MimoSeries_fiona BC:C6:DB:9F:1A:08 Nokia 01-24 08:45 01-24 09:48
OFFLINE bridge Fiona VAP0_1 MimoSeries_fiona BC:C6:DB:9F:1A:08 Nokia 01-24 08:45 01-24 09:48
OFFLINE bridge Fiona VAP0_1 MimoSeries_fiona BC:C6:DB:9F:1A:08 Nokia 01-24 09:22 01-24 09:48
OFFLINE bridge Fiona VAP0_2 Tet_holiday BC:C6:DB:9F:1A:08 Nokia 01-24 09:30 01-24 09:48
OFFLINE bridge Fiona VAP0_1 MimoSeries_fiona BC:C6:DB:9F:1A:08 Nokia 01-24 09:34 01-24 09:48
OFFLINE bridge Fiona VAP0_2 Tet_holiday BC:C6:DB:9F:1A:08 Nokia 01-24 09:37 01-24 09:48
OFFLINE bridge Fiona VAP0_2 Tet_holiday BC:C6:DB:9F:1A:08 Nokia 01-24 09:39 01-24 09:48
OFFLINE bridge Fiona VAP0_1 MimoSeries_fiona BC:C6:DB:9F:1A:08 Nokia 01-24 09:39 01-24 09:48
OFFLINE bridge Fiona VAP0_2 Tet_holiday BC:C6:DB:9F:1A:08 Nokia 01-24 09:46 01-24 09:48
OFFLINE bridge Fiona VAP0_1 MimoSeries_fiona BC:C6:DB:9F:1A:08 Nokia 01-24 09:48 01-24 09:48
OFFLINE bridge Fiona VAP0_2 Tet_holiday 00:37:6D:62:F6:C4 MurataMa 01-24 09:51 01-24 09:52
OFFLINE bridge Fiona VAP0_2 Tet_holiday 00:37:6D:62:F6:C4 MurataMa 01-24 09:52 01-24 09:52

(Some of the screenshots may appear different than what you see because of updates to the APc.)


AP Controller v1.00
Network : CP3
Logout
Discovery
Create Network
Network
Management
Users
Upgrade
Account
Hotspot
Documentation
Feedback
Status Mode AP'S Name Vap SSID Host IP Address MAC Address Brand Upload Download Total Check-in Check-out
OFFLINE Bridge Mi7 VAP0_1 M777 90:18:7C:F0:7C:AE SamsungE 1 05-08 07:39 05-08 08:09
OFFLINE Bridge Mi7 VAP0_1 M777 90:18:7C:F0:7C:AE SamsungE 1 05-08 08:09 05-08 08:38
OFFLINE Bridge Mi7 VAP0_1 M777 90:18:7C:F0:7C:AE SamsungE 1 05-08 08:38 05-08 09:07
OFFLINE Bridge Mi7 VAP0_1 M777 90:18:7C:F0:7C:AE SamsungE 1 05-08 09:08 05-08 09:37
OFFLINE Bridge Mi7 VAP0_1 M777 90:18:7C:F0:7C:AE SamsungE 1 05-08 09:37 05-08 10:06
OFFLINE Bridge Mi7 VAP0_1 M777 90:18:7C:F0:7C:AE SamsungE 1 05-08 10:06 05-08 10:36
OFFLINE Bridge Mi7 VAP0_1 M777 90:18:7C:F0:7C:AE SamsungE 1 05-08 10:36 05-08 10:57
OFFLINE Bridge Mi7 VAP0_1 M777 90:18:7C:F0:7C:AE SamsungE 05-08 10:58 05-08 10:59
OFFLINE Bridge Mi7 VAP0_1 M777 90:18:7C:F0:7C:AE SamsungE 05-08 11:01 05-08 11:01
OFFLINE Bridge Mi7 VAP0_1 M777 90:18:7C:F0:7C:AE SamsungE 05-09 00:54 05-09 00:54
OFFLINE Bridge Mi7 VAP0_1 M777 B4:07:F9:87:85:BC SamsungE 1 05-09 00:55 05-09 01:56
ONLINE Bridge Mi7 VAP0_1 M777 B4:07:F9:87:85:BC SamsungE 2 05-09 01:56
ONLINE Bridge Mi7 VAP0_2 M888 90:18:7C:F0:7C:AE SamsungE 2 05-09 03:32
Search
Status : All Status
MAC Address :
Display
Period : 1 Day
Display

Section 8: The [Upgrade] Page

In the [Upgrade] page, you can upgrade the firmware of the APc using the “APc Upgrade” tab or upgrade the firmware of the APs using the “AP Upgrade” tab.

8.1 APc Upgrade

It is recommended to first “Export APs” from the [Management] page, and download the .csv file. This would make it easy to import the same APs after the APc upgrade.

The first page that is displayed in the [Upgrade] page belongs to the “APc Upgrade” tab.

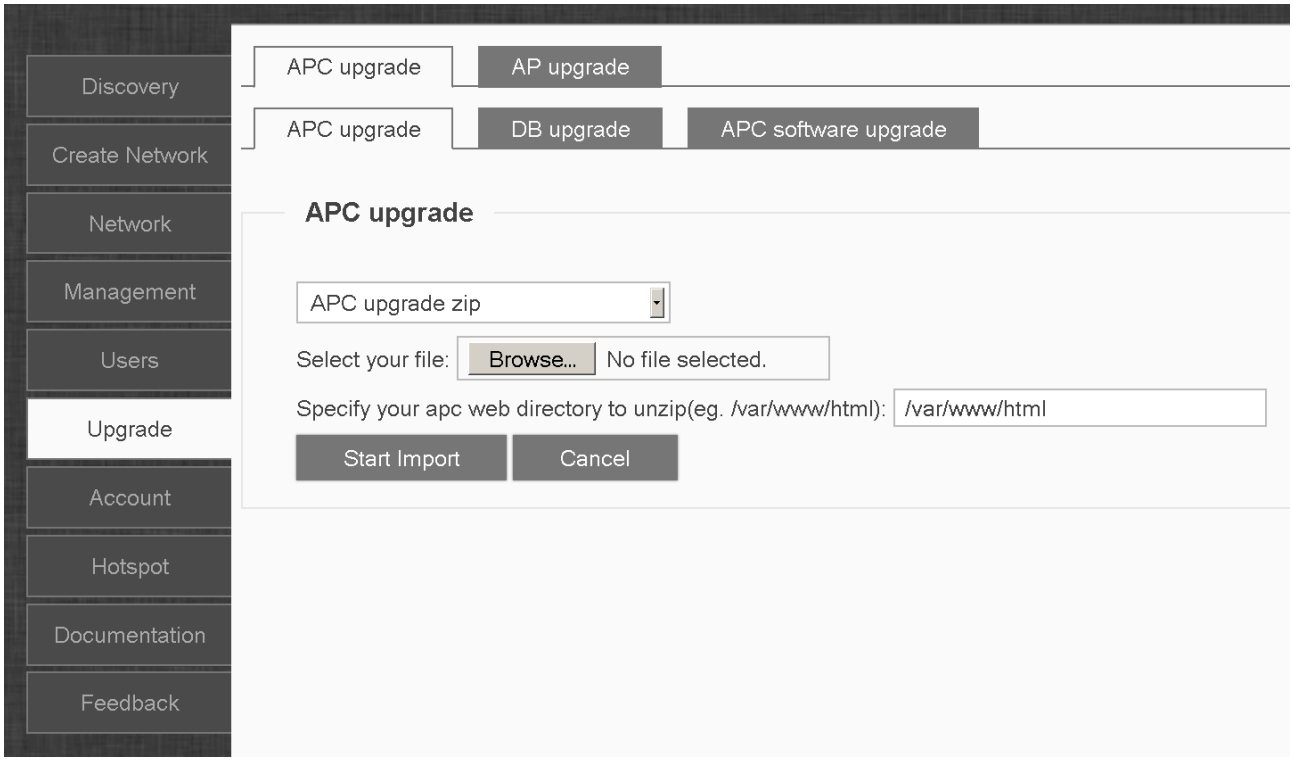


Figure 23: The [Upgrade] page.

This is where the firmware of the APc can be upgraded. Ideally, the APc should not be applying settings to the APs while doing the APc upgrade. In the [Management] page, make sure that the Status icon of the APs do not show the orange coloured text “Applying”. Otherwise, the affected parameters would take a longer time to be updated.

Select your file: You may browse for the required file “apc.zip”. Please make sure the filename is “apc.zip”.

Depending on the “apc.zip” file, the APc can be changed to either of these two versions:

- **Logo**: This has the Compex Logo and it does not require a license i.e. it is free for life.
- **License**: This does not have the Compex Logo and it has a trial license with an expiry date.

Specify your apc web directory to unzip (e.g. /var/www/html): By default, the directory path to place the uploaded file is “/var/www/html”.

Once the file is selected, please click “Start Import” to upload the file to the APc.

The database upgrade is performed automatically with the APc upgrade.

The web page would start processing. It may take half a minute. The web page would then show the message “Database upgrade successful”. Please click the “OK” button.

The APc upgrade is now completed.

It was found that for some cases, it is necessary to reset the APc after the APc upgrade. This is because the database had changed. Please click “Reset” in the [Account] page. You would have to create an APc network again. Following that, you may “Import APs” using the .csv file exported earlier.

Otherwise, if no reset is required, please follow this procedure:

After the APc upgrade, click “Logout”, press F5 / refresh, and then login again.

8.2 Older Method of APc Upgrade for APc

For the older version of the APc, v1.00, there is no “APc Upgrade” tab in the [Upgrade] page. Therefore, please refer to the following subsections to upgrade the APc. Also, if there are any problems with the “APc Upgrade” function on the APc web page, the following method would have to be used.

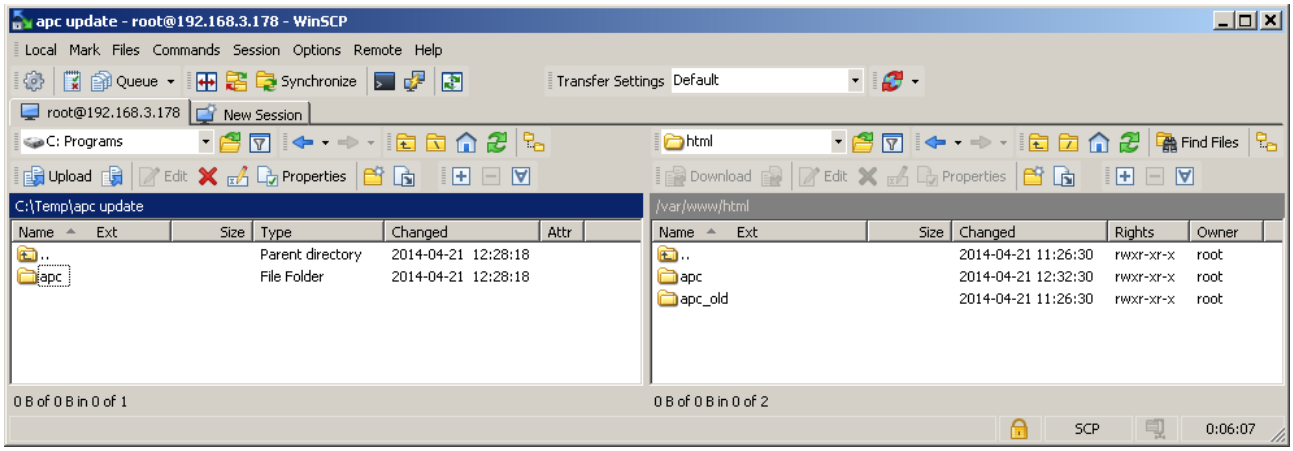
8.2.1 Upgrading the APc using WinSCP

The APc upgrade can be accomplished by replacing a certain folder called 'apc' in the APc's Linux file directory:

- \var\www\html\apc

A Secure Copy (SCP) program such as WinSCP can be used. The existing folder can be renamed to 'apc_old_01' for example, and the new 'apc' folder should be copied in.

Please make sure that the path is correct so that the AP discovery can work.



You would need to change the permissions of two folders. This can be done with a Secure Shell (SSH) program such as PuTTY. First log in to the APc's Linux shell using PuTTY.

Run the following commands:

- **`chmod -R 755 /var/www/html/apc`**
- **`chmod -R 777 /var/www/html/apc/storage/uploads`**
- **`reboot`**

The APc does not need to be installed again. Initialization is not needed (Section 2.5 *Perform Initialization by Running Three Scripts*). The settings in the APc are also retained.

If the permissions were not changed, when you view the Radio Settings, the page would not show, and it would say “can't open file”.

Next, reset the APc after the APc upgrade because the database has changed. Please click “Reset” in the [Account] page. You would have to create an APc network again. Following that, you may “Import APs” using the .csv file exported earlier.

8.2.2 Updating the APc License using WinSCP

When the license is expired, please upload the license file “License.txt” under the directory of /var/www/html/apc/

The WinSCP program can be used.

You would need to change the permissions of this file. This can be done with an SSH program such as PuTTY. First log in to the APc's Linux shell using PuTTY.

Run the following command:

- **`chmod -R 755 /var/www/html/apc/License.txt`**
- **`reboot`**

The license file may also be included inside a new 'apc' folder that you receive. You can follow the steps in the previous section to update the APc. The new license file would be used automatically.

8.3 AP Upgrade

The APc lets you upgrade multiple selected APs concurrently.

The SNMPv3 is used to manage the upgrade process.

The FTP protocol is used to transfer the firmware image to the APs.

The steps for the firmware upgrade are as follows:

8.3.1 Place Firmware Image on the APc's FTP Server

In Section 2.5.3 *Run the Script for 'ftp'*, the process for creating the FTP server on the APc was described. For convenience, it is repeated here.

In the Linux terminal, enter the following command:

- **`/bin/ftp.init.sh`**

Creating username and password for FTP server:

- Type username: ftpuser (for example)

Changing password for user ftpuser:

- New password: ftppass (for example)

Once the username and password are created, a new folder is created in the /home directory:

- /home/ftpuser/ (for example)

Firmware image files can be placed in the FTP server of the APc. Alternatively, any other FTP server can be used.

A secure shell (SSH) program such as WinSCP can be used to upload new firmware image files into this directory:

- /home/ftpuser/ (for example)

8.3.2 Enter the settings for the FTP

The fields on the [Upgrade] page and an example of the entries are as follows.

- FTP IP : 192.168.3.178 (This is the IP address of the APc.)
- FTP PORT : 21 (default)
- FTP Username : ftpuser (for example)
- FTP Password : ftppass (for example)
- FTP File Type : 1 (default)
- FTP File Name : wpj344.img (for example)

8.3.3 Select the Boards

On the [Upgrade] page, you can select multiple boards for upgrading at the same time. The selected boards should be of the same model e.g. WPJ344 because the firmware image is for a certain model only.

8.3.4 Press the Upgrade Button

Next, press the “Upgrade” button. On the following page, you can click the “Download” button for individual APs. The APc then sends the SNMP command to each AP to download the firmware.

Once each AP has downloaded the firmware, the “Upgrade” button would appear for this AP.

Please make sure that the communications between your PC and the APc are not disrupted by the upgrading process, because you have to click the buttons in the browser.

It is recommended to click “Upgrade” for the AP farthest from the gateway first. This is because while an AP is upgrading, all communications on this AP would be stopped. By using this method, all the APs can then be upgraded at the same time.

Finally, each AP sends back the status to the APc, whether the firmware upgrade was successful or unsuccessful.

If there were any problems in the upgrade process, the red words “Upgrade issue!” would show up. This is because the AP did not send the upgrade success message to the APc. Please mouse over the red words to see the details in the infotip.

If the upgrade was carried out successfully, the green words “Upgrade success!” would show up.

Section 9: The [Account] Page

In the [Account] page, you can edit the settings for Password, Email, and SNMP. You can also perform a reset of the APc.

9.1 Account Settings – Password

You can change the password for the APc configuration web page by filling in:

- Username (default: admin)
- Old Password (default: password)
- New password
- Confirm Password

9.2 Account Settings – Email Address

Here, you can change the email address for the APc by filling in:

- Current Email (default: none)
- New Email
  - Currently "+" in the email address is not supported here. However, "+" can still be used in the email address in the [Network] page.
- Confirm Email

This email address would be auto-filled when you are in the [Create Network] page.

If you forget the password for the APc login, you need to provide your APc account username and email address to reset the password.

9.3 SNMP Settings

This section describes the SNMP parameters used by the APc and the AP.

9.3.1 APc SNMPv3 Settings

Currently, this section may not be shown because these settings cannot be changed:

SNMPv3 Username: "admin"

SNMPv3 Auth Password: "apc0ntr0ll3r"

SNMPv3 Privacy Password: "apc0ntr0ll3r"

9.3.2 AP SNMP Settings

Currently, this section may not be shown because these settings cannot be changed:

SNMPv3 Username: “admin”

SNMPv3 Auth Password: “password”

SNMPv3 Privacy Password: “password”

Write Community: “private”

Read Community: “public”

9.4 Reset

Reset to default: This button allows you to reset the APc to its factory default state. All the APc settings would be deleted. Hotspot plans and user accounts are cleared as well. Therefore it is recommended to disable the Hotspot in the Hotspot AP first.

Section 10: The [Hotspot] Page

In the [Hotspot] page, you can see the following tabs:

Prepaid, Postpaid, Office, Guest, Report.

10.1 Office

The Office Plan is useful for managing the employee's use of the Internet.

10.1.1 Plan List

In this page, you can create and view Hotspot plans.

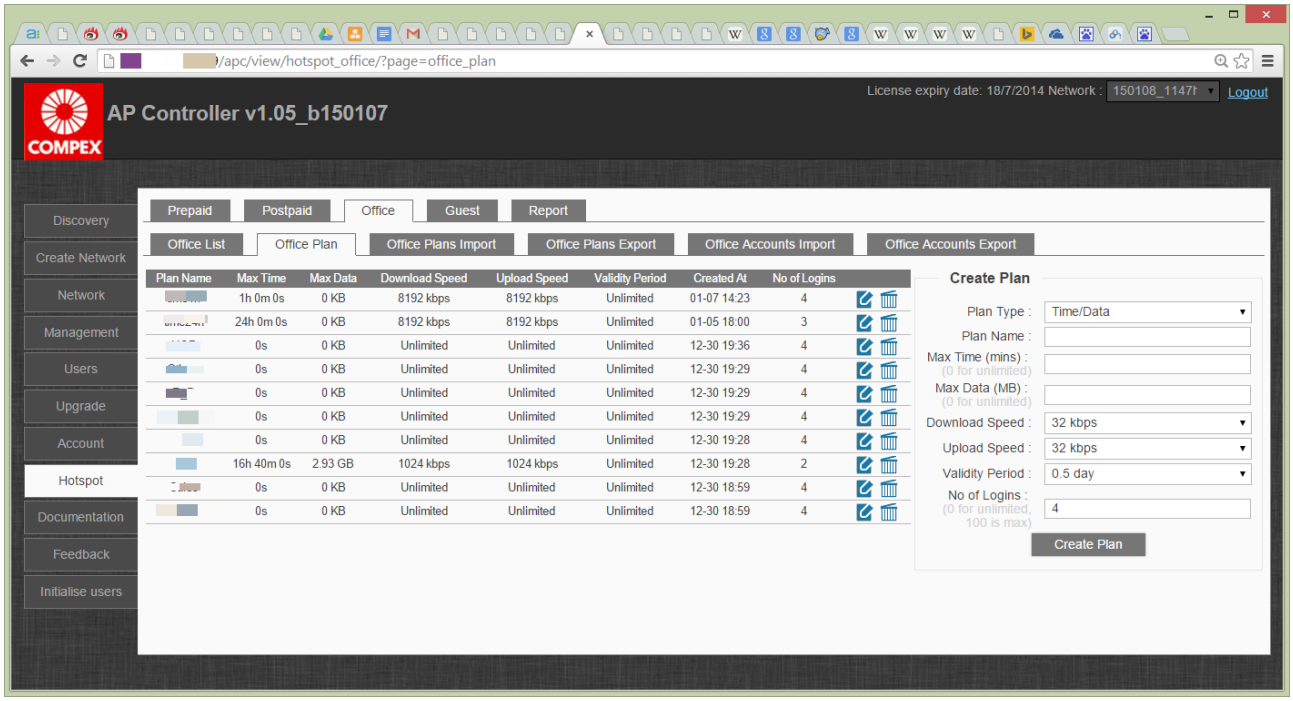


Figure 24: The Office Plan tab.

To create a hotpot plan, you may set the plan details under the “Create Plan” section:

- Plan Type (0, 1, or 2)
  - 0 for Data
  - 1 for Time
  - 2 for Time/Data (Recommended)
- Plan Name (no spaces)
- Max Time (mins) (0 for Unlimited)

- Max Data (MB) (0 for Unlimited)
- Download Speed (32 kbps, 64 kbps, 128 kbps, 256 kbps, 384 kbps, 512 kbps, 784 kbps, 1 Mbps, 1.5 Mbps, 2 Mbps, 4 Mbps, 8 Mbps, or Unlimited)
- Upload Speed (32 kbps, 64 kbps, 128 kbps, 256 kbps, 384 kbps, 512 kbps, 784 kbps, 1 Mbps, 1.5 Mbps, 2 Mbps, 4 Mbps, 8 Mbps, or Unlimited)
- Validity Period (0.5 day, 1 day, 1.5 day, 2 day, 2.5 day, 3 day, 3.5 day, 4 day, 4.5 day, 5 day, or Unlimited (Recommended))
- Number of concurrent logins (0 for unlimited, 100 is max)

The created plans are shown in the table.

10.1.2 Account List

In this page, you can create and view Hotspot user accounts.

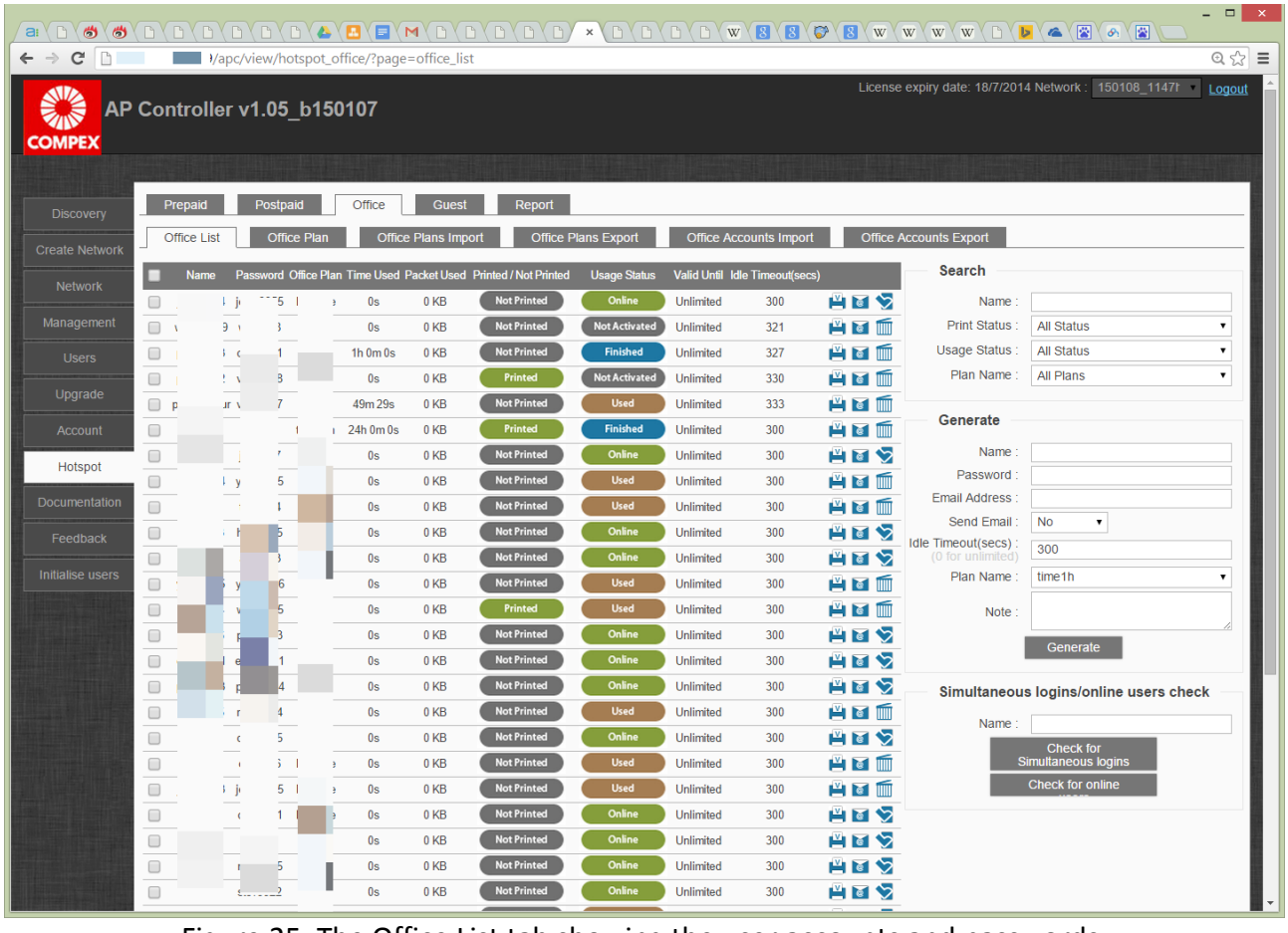


Figure 25: The Office List tab showing the user accounts and passwords.

To generate a user account, please fill in the details under the “Generate” section:

- UserName (no spaces)

- Password (no spaces)
- Email Address
- Send Email to user about her account once created (Yes or No)
- Idle Timeout (in seconds, 0 for unlimited)
- Plan Name (to select from the dropdown box)
- Note

Once done, click on the “Generate” button.

The Hotspot user accounts are shown in the table.

10.1.3 Plan Import ()

(Note that the number of concurrent logins are not imported in the current version.)

The .csv file would follow the details in the “Create Plan” section.

For example, one row of the .csv file could be: 2,officeplan1,60,1024,784,512,3,88

The Upload/Download Speed should be given in terms of kbps.

Value in .csv file	Upload/Download Speed
32	32 kbps
64	64 kbps
128	128 kbps
256	256 kbps
384	384 kbps
512	512 kbps
784	784 kbps
1024	1 Mbps
1536	1.5 Mbps
2048	2 Mbps
4096	4 Mbps
8192	8 Mbps
102400	Unlimited

10.1.4 Plan Export ()

Note that the units may be different than the “Plan Import” in the current version.

10.1.5 Account Import

The .csv file should follow the details in the Account “Generate” section.

The columns are:

UserName,Password,Email,0,PlanName,Note,IdleTimeout

For example, one row of the .csv file could be:

wtau0123,wtap0123,pm@gmail.com,0,officeplan1,Note WTA 0123,600

Note that the PlanName e.g. “officeplan1” must exist, otherwise an error message would be thrown up.

(For older versions, please make sure that there are no blank lines in the .csv file because it may cause database corruption.)

The APc would not send out the emails to the users at this stage. Later, you can select the users and click the “Send Email” button. (For older versions, it may take 20 minutes to send to 300 users automatically and the APc web page cannot be accessed at this time. To cancel, reboot the APc. Existing users would be logged in again automatically.)

10.1.6 Account Export

The .csv file follows the details in the Account “Generate” section.

This file can be used for “Account Import”.

10.2 Guest

In order to use the “Agreement (RADIUS Required)” Hotspot plan, please create a plan called “agreement” and a user account with username “agreement” and password “password”.

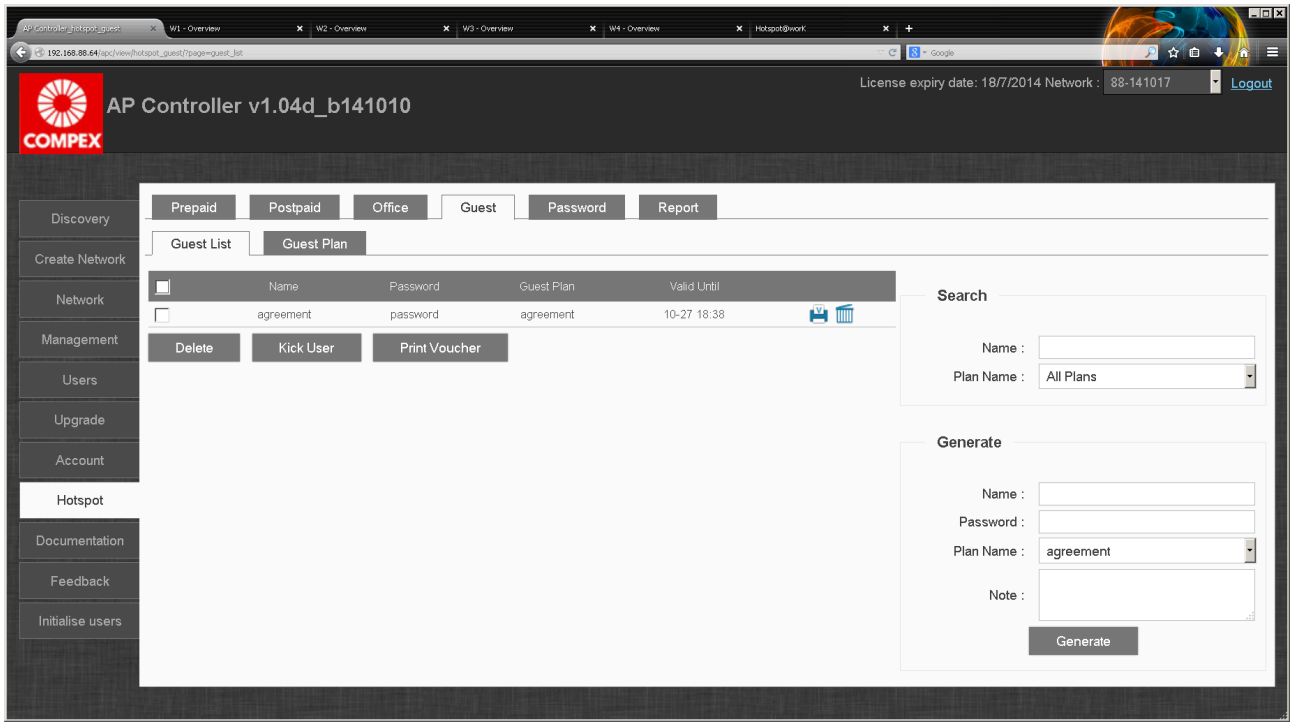


Figure 26: To use the “Agreement (RADIUS Required)” Hotspot mode, create a user account “agreement”.

To use the “Password (RADIUS Required)” Hotspot plan, please edit the existing “pwdplan” in the Guest tab with the upload/download speed limitations and concurrent logins limitation.

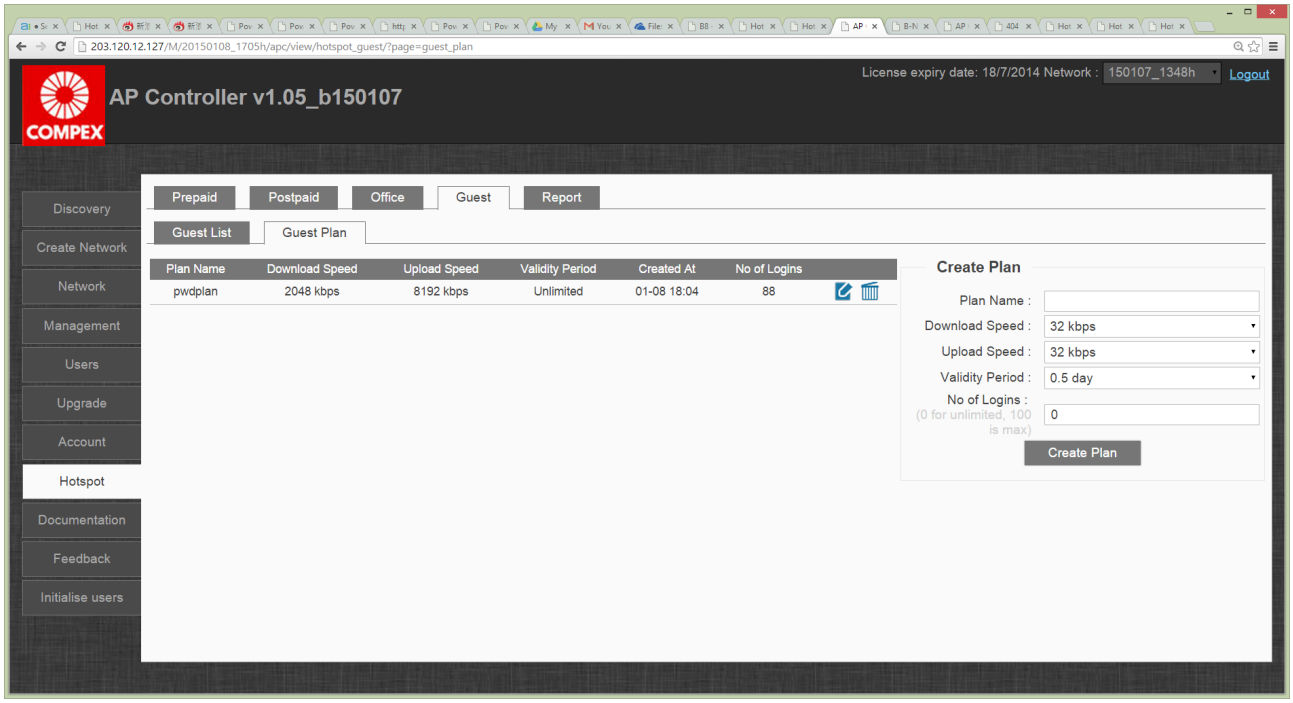


Figure 27: Please edit the “pwdplan” in the Guest tab to use the Password Plan.

Next, create a user account with username “passwordmode” and with a password of your choice.

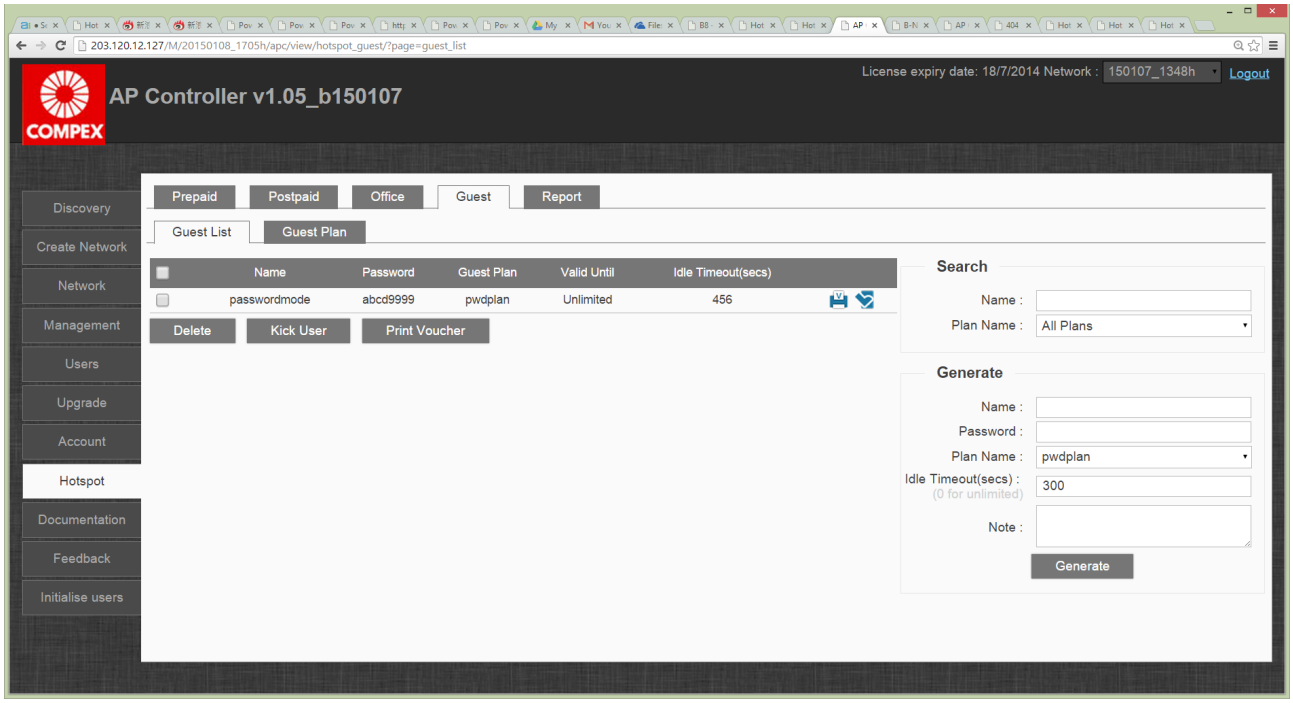


Figure 28: The “passwordmode” username with a password “abcd9999”.

The user would then only enter the password e.g. “abcd9999” to login to the Hotspot.

Other than these two special plans (“agreement” and “pwdplan”), other plans can be created. All plan names must be unique.

Other than these two special usernames (“agreement” and “passwordmode”), other user accounts can be created. All usernames must be unique. These other users can login using their usernames and passwords when the “User Name + Password (RADIUS Required)” Hotspot option is selected.

10.3 Prepaid

This tab is for the prepaid users.

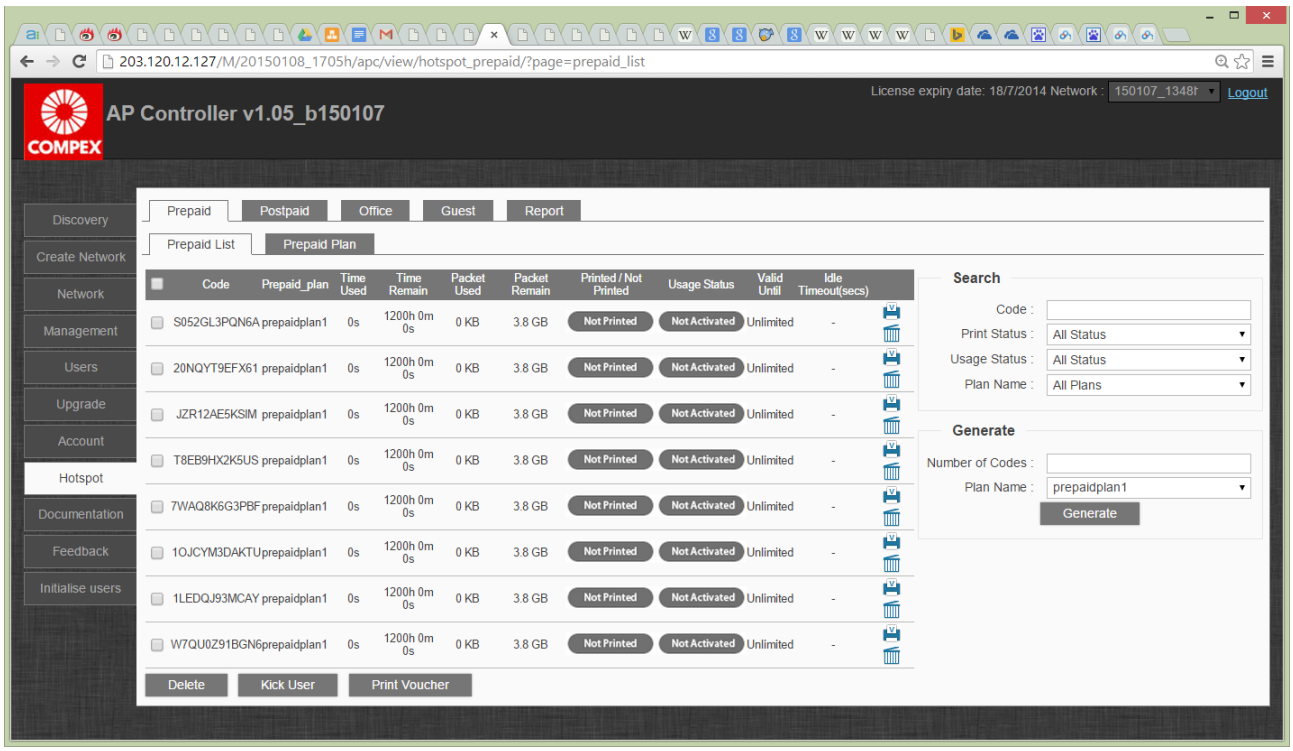

203.120.12.127/M/20150108_1705h/apc/view/hotspot_prepaid/?page=prepaid_list
AP Controller v1.05_b150107
License expiry date: 18/7/2014 Network : 150107_1348
Logout
Discovery
Create Network
Network
Management
Users
Upgrade
Account
Hotspot
Documentation
Feedback
Initialise users
Prepaid
Postpaid
Office
Guest
Report
Prepaid List
Prepaid Plan
Code
Prepaid_plan
Time Used
Time Remain
Packet Used
Packet Remain
Printed / Not Printed
Usage Status
Valid Until
Idle Timeout(secs)
S052GL3PQN6A prepaidplan1 0s 1200h 0m 0s 0 KB 3.8 GB Not Printed Not Activated Unlimited -
20NQYT9EFX61 prepaidplan1 0s 1200h 0m 0s 0 KB 3.8 GB Not Printed Not Activated Unlimited -
JZR12AE5KSIM prepaidplan1 0s 1200h 0m 0s 0 KB 3.8 GB Not Printed Not Activated Unlimited -
T8EB9HX2K5US prepaidplan1 0s 1200h 0m 0s 0 KB 3.8 GB Not Printed Not Activated Unlimited -
7WAQ8K6G3PBF prepaidplan1 0s 1200h 0m 0s 0 KB 3.8 GB Not Printed Not Activated Unlimited -
1OJCYM3DAKTU prepaidplan1 0s 1200h 0m 0s 0 KB 3.8 GB Not Printed Not Activated Unlimited -
1LEDQJ93MCAY prepaidplan1 0s 1200h 0m 0s 0 KB 3.8 GB Not Printed Not Activated Unlimited -
W7QU0Z91BGN6 prepaidplan1 0s 1200h 0m 0s 0 KB 3.8 GB Not Printed Not Activated Unlimited -
Delete
Kick User
Print Voucher
Search
Code :
Print Status : All Status
Usage Status : All Status
Plan Name : All Plans
Generate
Number of Codes :
Plan Name : prepaidplan1
Generate

Figure 29: The Prepaid User List tab.

In the “Prepaid Plan” tab, you may create plans in the same manner as in the “Office plan” tab.

In the “Prepaid List” tab, you may generate a number of codes using the “Generate” section.

The user will login using the Code as her username as well as her password.

10.4 Postpaid

In the “Postpaid Plan” tab, the postpaid users are shown.

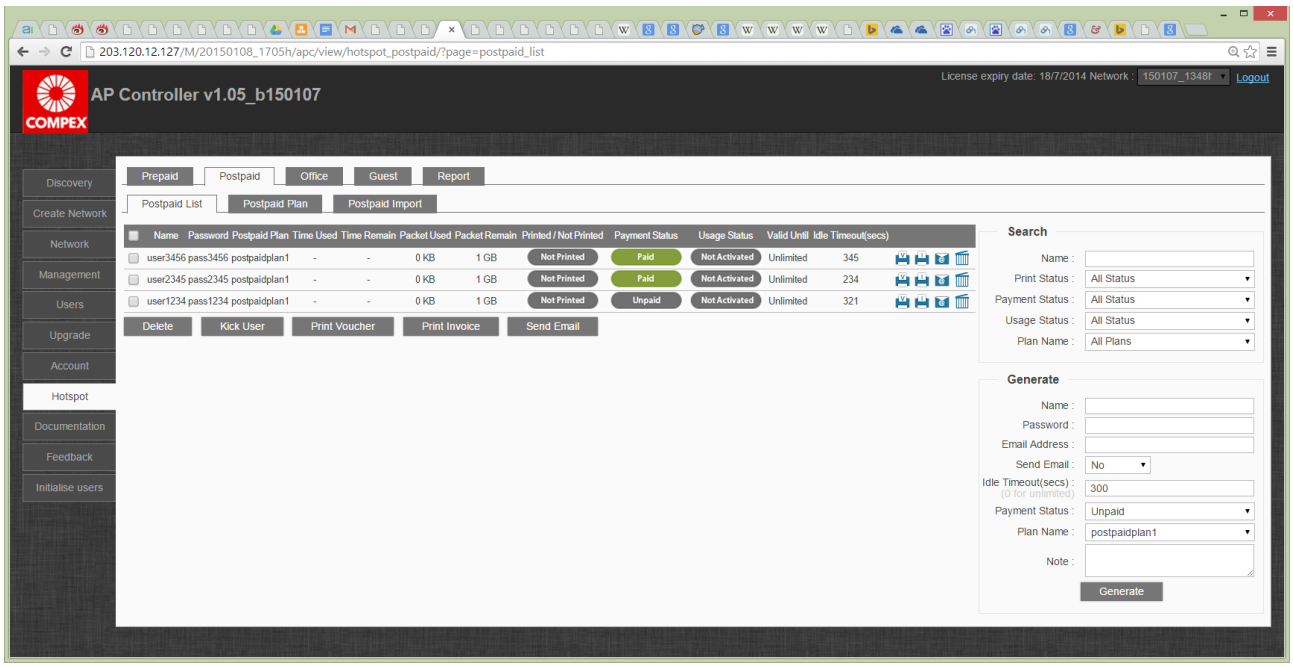


Figure 30: The Postpaid List tab.

For the “Postpaid Import”, you may upload a comma separated values (.csv) file of the Postpaid Hotspot plans with the column details as follows:

- Plan Type (0 or 1)
  - 0 for Data
  - 1 for Time
- Plan Name (no spaces)
- Max Time (mins) (0 for Unlimited)
- Max Data (MB) (0 for Unlimited)
- Download Speed (32 kbps, 64 kbps, 128 kbps, 256 kbps, 384 kbps, 512 kbps, 784 kbps, 1 Mbps, 1.5 Mbps, 2 Mbps, 4 Mbps, 8 Mbps, or Unlimited)
- Upload Speed (32 kbps, 64 kbps, 128 kbps, 256 kbps, 384 kbps, 512 kbps, 784 kbps, 1 Mbps, 1.5 Mbps, 2 Mbps, 4 Mbps, 8 Mbps, or Unlimited)
- Validity Period (0.5 day, 1 day, 1.5 day, 2 day, 2.5 day, 3 day, 3.5 day, 4 day, 4.5 day, 5 day, or Unlimited)
- Price

For example, one row of the .csv file could be: 1,postpaidplan1,60,0,128,8096,5,6

10.5 Report

In the Hotspot Report tab, the history of users are shown with Online/Used/Finished Status.

The details are UserName, Plan Type, Plan Name, IP Address, MAC Address, Check-in Time, Last Seen On (check-out time), Downloaded MB, and Uploaded MB.

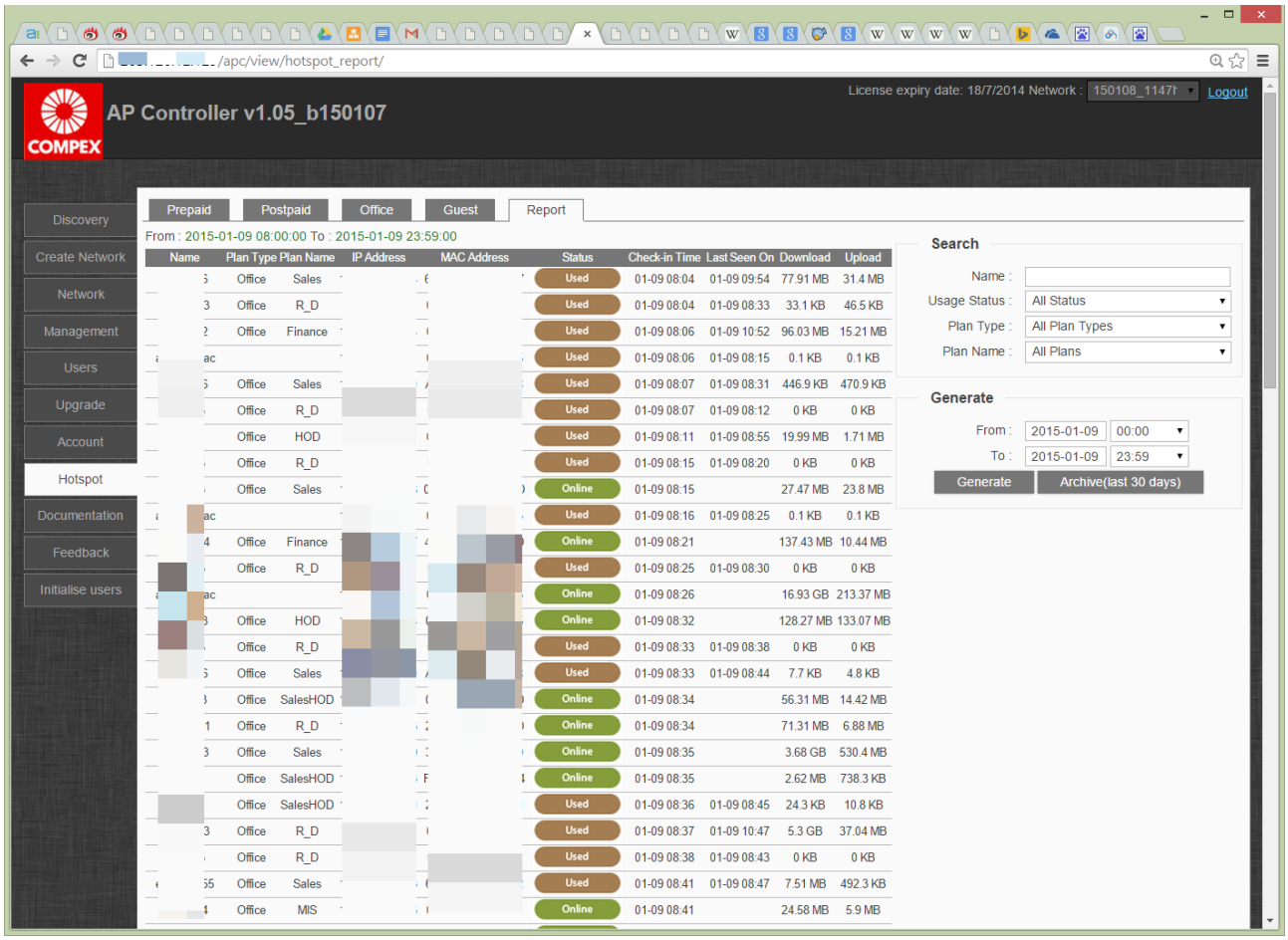


Figure 31: The Hotspot Report tab.

The date range of the history can be selected.

10.6 Possible Setup Scenario of Hotspot with Mesh APs and APc

The following network topology diagram shows an example how the mesh APs can be set up with the Hotspot controlling the Internet traffic.

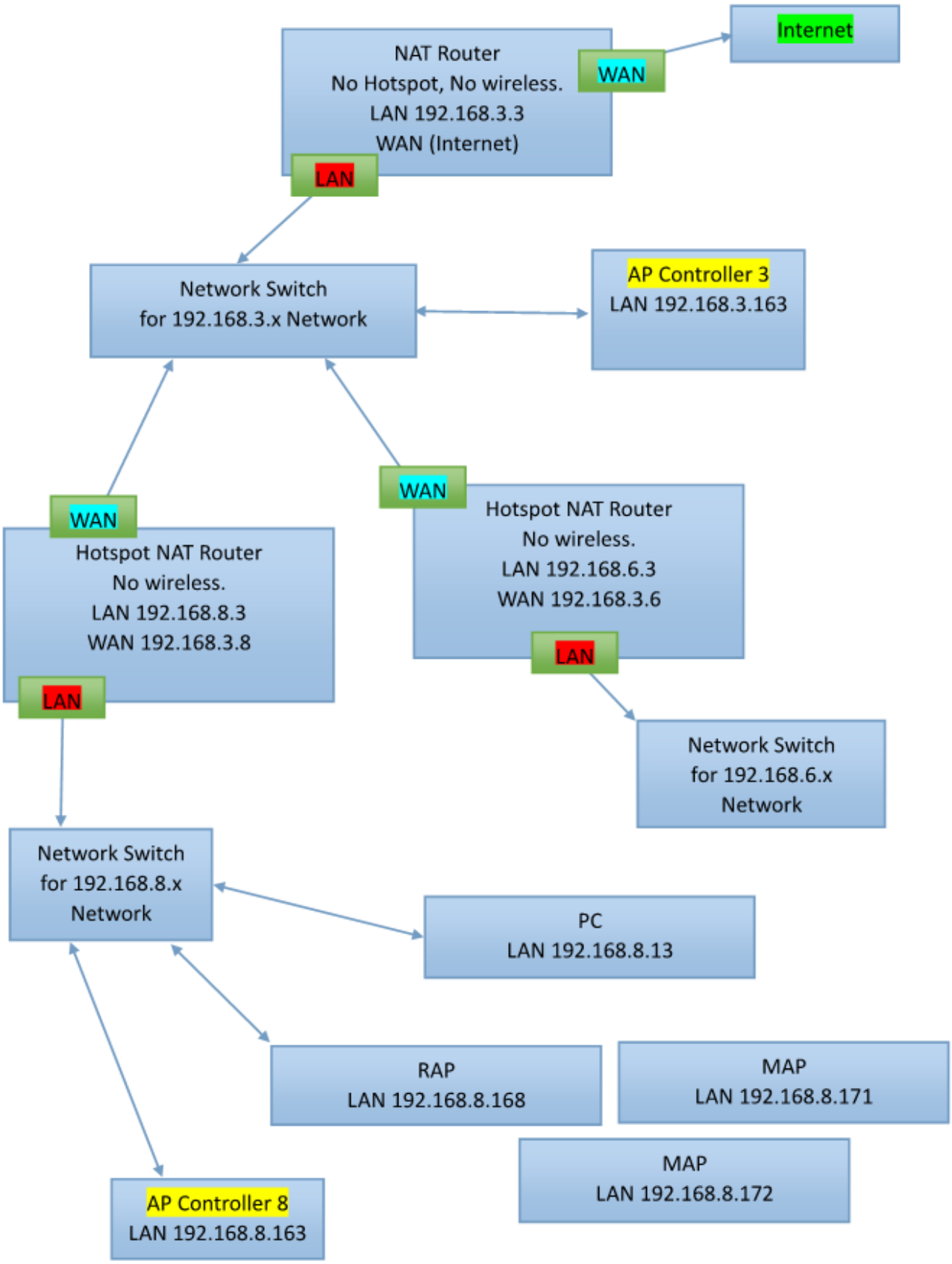


Figure 32: Network topology diagram showing Hotspot with mesh APs and APc

In the figure, “AP Controller 3” is on the WAN side of both the “Hotspot NAT Router 192.168.8.3” and the “Hotspot NAT Router 192.168.6.3”. Therefore, it is able to control both of these Hotspots.

The “AP Controller 8” is on the same LAN network as the “Hotspot NAT Router 192.168.8.3”. This is also a possible position for the APc. It would be able to control this Hotspot if this router was configured to use this APc. It cannot control the “Hotspot NAT Router 192.168.6.3” because they are on different networks.

The diagram also shows that the RAP and MAPs are on the same LAN network 192.168.8.x.

The “AP Controller 3” is also able to control these mesh APs because the mesh APs are able to ping to the APc. This can be done by simply adding the APc's IP address into the Walled Garden of the “Hotspot NAT Router 192.168.8.3”.

Section 11: Troubleshooting

This section describes the troubleshooting or debugging steps that can be taken.

11.1 To Check: No Spaces in any Field

Currently the APc web page does not support any spaces in any of the fields. This is because spaces are interpreted as commands. Please check that all parameters and names are without spaces. You may use an underscore "**_**" or a dash "**-**" to replace a space.

11.2 Use ping to Check for Connection

The configuration web page for the APc would not be able to show up if the APc and your computer are not connected.

First check whether the APc and your computer are connected on the same network by running the ping command to ping the IP addresses of the APc. Alternatively, type the following in the APc's Linux terminal:

- **`ping 192.168.3.77`** (if your computer's IP address is 192.168.3.77 for example.)

They should be able to give the ping responses.

If not, check if the cable connections are loose.

If using a Windows computer, you should run the command **`arp -d *`** if the network configuration has changed. This is to delete the address resolution protocol (ARP) table in Windows as it may not update fast enough.

The ping command can also be used to check if an AP is connected on the same network.

11.3 Run AP Command to Check-In Manually

If you are able to get ping responses from the APc and AP, they are connected but the AP may still not be able to check-in to the APc. The result is that the AP shows up as 'OFFLINE' on the APc.

The following is the command that can be run in the AP's Linux shell to allow it to check-in manually:

- **`/lib/faito/update_settings_nodes.sh 1minuteUd`**

The SSH program PuTTY can be used to access the AP's Linux shell.

11.4 To Create AP with MAC Address of wifi0

If you create an AP using the “Create AP” page with a wrong MAC address, the AP would not be able to check-in to the APc.

The MAC address of the AP's onboard radio (wifi0) should be used. This MAC address is also written on the product box.

More information can be found in Section Error: Reference source not found *Error: Reference source not found*.

11.5 To Create AP with Correct Model

When using the “Create AP” page, if any of the following fields are not correct, the AP would not be able to check-in and the Model would show in red words with “!?”

- PCB
- Radio 1
- Radio 2

In this case, you would have to delete the AP in the [Management] page with the “Delete” button, then add the AP again.

11.6 The World Map needs an Internet Connection

Either the World Map or a Custom Map can be used to place the APs. The World Map uses the Google Map. If using the World Map, the following applies.

The World Map in the [Management] page may not show up in the browser if your computer is not connected to the internet. A small cached map may appear instead. You would also not be able to change the position of an AP when you click “Settings”.

Your computer would need to have Internet connection. This is to allow the Google Map to be downloaded and shown in the browser.

11.7 Reset

When there are problems with the APc, you can reset it back to the default settings where there are no APc networks.

This can be done in the [Account] page, by clicking on the “Reset” button.

The APc does not need to be installed again.

You would have to create an APc network again and then add APs.

11.8 Error: ionCube PHP Loader

When you access the APc using an Internet browser, you may see this error message in the web page:

Site error: the file **/var/www/html/apc/index.php** requires the ionCube PHP Loader ioncube_loader_lin_5.3.so to be installed by the website operator. If you are the website operator please use the ionCube Loader Wizard to assist with installation.

Solution Summary:

This problem occurs in the older version v1.00 of the APc.

Please check this file in the APc: /etc/selinux/config

To make sure that you set: SELINUX=disabled

Solution Details:

The details of solving this problem is as follows.

First login to the APc's Linux shell. This may be done locally at the APc hardware or remotely by using PuTTY.

The “/etc/selinux/config” is not a script. It is a file that stores configuration settings.

Therefore, the command to be used is:

- **`vi /etc/selinux/config`**

This would open up the VIM text editor in Linux. The correct content of the file should be:

```
SELINUX=disabled

SELINUXTYPE=targeted
```

You would see the incorrect line:

```
SELINUX=enforcing
```

You are currently in the view mode of VIM.

- Please press “i” to enter the editing mode.
- Please use the arrow keys to move the cursor.
- Next, delete “enabled” and replace with “disabled”.
- Then press “ESC” to get back to the view mode of VIM.
- Type “:w” and Enter to write the changes to the file.

- Type ":q" and Enter to exit the VIM editor.
- (If you made any mistakes, type ":q!" and Enter to exit the VIM editor without saving.)

After you make the change, please enter this command to reboot the APc:

- **`reboot`**

Alternative Solution:

Instead of editing the file using "vi" in Linux, the WinSCP program can be used to edit the file remotely from a Windows PC.

11.9 License File Error

Instead of the APc Login page, you may see:

Fatal error: The license file /var/www/html/apc/License.txt for /var/www/html/apc/index.php has expired. in Unknown on line 0

This means that the License file has expired.

Please follow the steps in Section 8.2.2 *Updating the APc License using WinSCP* to update the License file.

Note: The new APc (from v1.02 onwards) with the Compex Logo does not require the License file.

11.10 Error: mysql_connect

When you access the APc's web page, instead of the login page, you may see this error message in the browser:

Warning: mysql_connect(): Access denied for user 'root'@'localhost' (using password: YES) in /var/www/html/apc/model/config.class.php on line 0 Error connecting to database: localhost

This means that you have not yet run the 'mysql' script. This is one of the three scripts that you would need to run to perform initialization.

Please refer to Section 2.5.2 *Run the Script for 'mysql'*.

11.11 Problem: [Discovery] Scan is Not Finding the AP

When running the Scan in the [Discovery] page, the APc may not be able to find the AP.

The problem may be due to SNMP passwords being changed. Currently the SNMP settings should not be changed. The default values are given in Section 9.3.1 APc SNMPv3 Settings and Section 9.3.2 AP SNMP Settings.

The future version of the APc would allow the change of the SNMP settings from the default values.

11.12 Problem: Custom Map uploaded but cannot display

This problem is due to the permissions of the upload folder.

Please run an SSH program such as PuTTY, login to the APc, and run the following command:

- **`chmod 777 /var/www/html/apc/storage/uploads`**
- **`reboot`**

Following that, please upload your custom map again.

11.13 Error: Device cannot check-in because model settings conflict with device model

In the Status table on the [Management] page, when you mouse over a model name displayed as red words, e.g. “WPJ344_2V !?”, you may see this error infotip:

- Device cannot check-in because model settings conflict with device model.

This could be because you disabled a radio on the AP, changing the model name. (In future revisions of the firmware, disabling a radio would not change the model name.) Similarly, you could have enabled a radio on the AP. Normally, the APc would automatically resolve this by changing the model name for check-in after some time. To quickly resolve this problem, please click “Settings” in the Status table to allow the APc to get the parameters from the AP. Then, please click the [Management] page again.

11.14 Problem: AP cannot check-in

First make sure that the AP can ping to the APc because this is a prerequisite.

In the AP's shell, enter:

- **`crontab -e`**

This will open a vi editor. If it is an older firmware it may show only:

```
root@PowerAP:~# crontab -e
*/1     *       *       *       * /lib/faito/every1minutes.sh
```

Either use the latest firmware or edit the file to:

```
root@PowerAP:~# crontab -e
*/1     *       *       *       * /lib/faito/every1minutes.sh
*/3     *       *       *       * /lib/faito/rescuel2tp.sh
```

When you see the line containing "`rescuel2tp`", please proceed to the following steps.

In the AP's shell, enter:

- **`ifconfig`**

There should be an interface called "`l2tp-avlan3316`" for the APc to communicate with the AP using the L2TP tunnel.

There is a tunnel to each AP. To restart the tunnel at the AP side, the commands are:

- **`/etc/init.d/xl2tpd restart`**
- **`/lib/faito/rescuel2tp.sh`**

To restart all the tunnels at the APc side, the command is:

- **`/etc/init.d/xl2tpd restart`**

The AP should be able to check-in now.

Helpful commands for debugging on the AP are:

- **`ping <APc IP address>`**
- **`ifconfig`**
- **`cat /tmp/Restart_xl2tp_log`**
- **`cat /tmp/l2tp/options.avlan3316`**
- **`uci show default`**
- **`uci show apc`** (to show the settings that the AP received from the APc)

Helpful commands for debugging on the APc are:

- **`ifconfig`**
- **`pidof nagios`**
- **`cat /tmp/xl2tpd/Restart_xl2tp_log`**
- **`ps -aux`**

11.15 Problem: AP can check-in but the APc cannot get the settings from the AP

The AP may show up as online, and when you click "Settings" to look at the "Radio Settings", you only see the blank settings, not the actual settings on the AP.

There are two possible reasons.

One is that the SNMP settings are not correct. The other possibility is that the APc database had changed during the previous APc Upgrade (by zip or WinSCP).

Regarding the SNMP settings (of username and passwords), the factory default settings already allow the communications between the APc and the AP.

There are two sets of SNMP settings: APc SNMP settings and AP SNMP settings. These two settings exist on both the APc and the AP, resulting in a total of 4 sections that can be configured. These settings are not transferable over the L2TP tunnel because of security reasons.

As for the problem of the database change during the APc Upgrade, the easiest way to resolve this is to do:

Export APs, Export Hotspot, (APc Upgrade), Reset APc, Import APs, Import Hotspot.

Section 12: Sending Feedback

In the [Feedback] page, you can send us a note by filling in the following fields:

- Name
- Email
- Phone
- Message

We would respond promptly.

Section 13: Nagios

The APc is based on Nagios. Therefore many types of status can be monitored as well. An alert plugin can be used for sending SMS. There is also support from the community.